Learning Community Trust

Data protection policy

Including trust-wide privacy notices

Date	November 2025
Version	3
Circulation	Public
Owner	Head of IT and Data
Date approved	November 2025
Approved by	Audit and Risk
Review date	August 2028
Status	Approved

Contents

Aims

The Learning Community Trust aims to ensure that all personal data collected about employees, young people, parents and carers, governors/trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individuals: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation • Safeguarding information
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Term	Definition
The Trust/Trust	When referring to the trust within this policy, this means the Learning Community Trust, central services and all academies and services the trust offers.
UK Data Protection Act	Where the term UK Data Protection Act is used in this policy it also UK Data Protection Act 2018/UK General Data Protection Regulations (GDPR) and the Data Use and Access Act 2025.

Legislation and related policies

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- Data Use and Access Act 2025 (DUAA 2025)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

This policy should be read in conjunction with other trust policies, such as information retention policy, acceptable use of IT agreement, IT security policy and other relevant polices and statutory guidance.

Data Controller

The trust processes personal data relating to parents and carers, young people, employees, governors/trustees, visitors and others, and therefore is a data controller. The person named as the day-to-day contact for the data controller is the Head of IT and Data.

The trust is registered under reference ZA285539 with the Information Commissioner's Office and has paid its data protection fee to the Information Commissioners Office, as legally required.

Roles and responsibilities

This policy applies to all employees employed by the trust, and to external organisations or individuals working on our behalf. Employees who do not comply with this policy may face disciplinary action. In addition, non-compliance with the UK Data Protection Act could constitute a criminal action.

Board of trustees

The board of trustees has overall responsibility for ensuring that the trust complies with all relevant data protection obligations.

Data controller/data protection lead

The trust is the data controller, but the name contact is the Head of Data and IT, who is the data controller on a day-to-day basis, and is responsible for ensuring this policy is implemented and understood across the trust.

The data controller will provide an annual report of activities to the risk and audit committee of the board of trustees.

As the data protection officer is outsourced, the named data controller will act as the trusts data protection lead. The data controller can be contacted through trust and academy website, but also, via dataprotection@lct.education.

Data protection officer

The data protection officer is responsible for overseeing monitoring the trusts compliance with data protection law and supporting the data controller to develop related policies and guidelines where applicable. The data protection officer can be contacted through the academy website, but also, via dpo@lct.education. This role is outsourced to a data protection officer as a service company.

Executive team

The executive team are responsible for monitoring the actions of the data controller/data protection lead and supporting the data controller/data protection lead, to ensure that data protection is a priority and is implemented consistently across the trust's academies.

Headteacher/principal

The headteacher/principal must ensure that the trust data protection policy is adhered to within their academy, working the with the information and data governance team, to ensure compliance.

Employees

Employees are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy and basis for processing as outlined in the information asset register
- Informing the trust of any changes to their personal data, such as a change of address
- Contacting the information and data governance team in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

GDPR principles

The UK Data Protection Act is supported by a set of 6 principles which must be adhered to whenever personal information is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal information.

The UK Data Protection Act principles relevant to the school state that personal information must:

- Be processed fairly, lawfully and transparently
- Obtained for a specified, explicit and legitimate purpose
- Be adequate, relevant and limited to what is necessary
- Be accurate and where necessary up to date
- Not be kept longer than is necessary
- Be handled ensuring appropriate security

There is a further principle called the accountability principle. This requires the trust to be able to clearly demonstrate their compliance with the UK Data Protection Act. The trust undertakes an annual exercise to ensure that the trust complies with this principle.

Individuals' rights

Individuals have rights under the UK Data Protection Act.

These include:

- The right to be informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right of data portability
- The right to object
- Rights related to automated decision making/profiling

If the trusts receive such a request on any of the above matters, they should seek advice from the information and data governance team as soon as the request is received, as they will liaise with the trust's data protection officer.

In most cases the request will constitute a subject access request. Please refer the subject access request section of this policy for further information.

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the trust can **fulfil a contract** with the individual, or the individual has asked the trust to take specific steps before entering a contract
- The data needs to be processed so that the trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the trust, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the trust (where the processing is not for any tasks the trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a young person) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Employees must only process personal data where it is necessary do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the trust's information retention policy.

Access and use of personal information

Access and use of personal information held by the trust, is only permitted by employees (temporary or permanent), governors/trustees, contractors, agents and anyone else processing information on the trust's behalf, for the purpose of carrying out their official duties. Use or access for any other purpose is not allowed. Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

Collecting personal information

When personal information is collected, for example on a questionnaire, survey or an application form, the 'data subject' (that is the person who the information is about) must be told. This is known as a privacy notice.

Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information. It must be made clear to the 'data subject' all the purposes that their information may be used for at the time the information is collected, via a privacy notice.

Conditions of processing

Article 6 – personal data

a. the data subject has given consent to the processing of their personal data for one or more specific purposes;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. is necessary for compliance with a legal obligation to which the controller is subject;
d. processing is necessary in order to protect the vital interests of the data subject;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 9 - special category data

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are manifestly made public by the data subject;
f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Disclosing personal information

Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

If personal information is given to another organisation or person outside of the trust, the disclosing person must identify the lawful basis for the disclosure and record their reasoning for using this basis. The disclosure of any information outside the trust must be approved by the data controller/data protection lead or the trust executive team in their absence.

This record as a minimum should include;

- a description of the information given
- the name of the person and organisation the information was given to
- the date
- the reason for the information being given
- the lawful basis

If an information sharing agreement exists, this should be adhered to when providing personal information to others. The agreement will detail the legal basis for disclosure.

In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive. Data minimisation should always be employed.

When personal information is given either externally or internally, it must be communicated in a secure manner, e.g. password protected/encrypted emails, special delivery or courier, etc.

Sharing personal data outside of the trust

- DO share personal data on a “need to know” basis and think about why it is legally to share data outside of the trust

- DO encrypt external emails, using Microsoft Purview Encryption when they contain personal data or any special category data

- DO be aware of "blagging". This is the use of deceit to obtain personal data from people or organisations. Seek advice through information and data governance team who will work with the data protection officer if there is any suspicion as to why the information is being requested or if there are concerns about the identity of the requester (e.g. if a request has come from a parent/carer but using a different email address than recorded on file)

- DO be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to digital, IT and data services – including the report function in Outlook

- DO NOT disclose personal data to contractors without consulting with the information and data governance team, unless a formal data sharing agreement is already is approved by the Head of IT and Data. This includes, for example, sharing personal data with an external marketing team to carry out a pupil recruitment event.

Sharing personal data within the trust

This section applies when personal data is shared within an academy or across the trust. Personal data must only be shared on a "need to know" basis.

The following are examples of sharing which are likely to comply with the data protection legislation:

- A teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil)
- Informing an exam invigilator that a particular pupil suffers from panic attacks
- Disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential)
- Employee OneDrive and emails, transfers with them when if/when they change place of work within the trust

The following are examples of sharing which are unlikely to comply with the data protection legislation;

- Disclosing personal contact details for a member of staff (e.g. their home address and telephone number, birthday) to other members of staff (unless the member of staff has given permission or it is an extreme emergency)
- Disclosing information about a young person to an agency teacher, which is beyond the information they need to keep the young person safe and educated.

Personal data may be shared to avoid harm, for example in child protection and safeguarding matters. Each academy has a child protection and safeguarding policy which should be referred to and training must include the sharing of information relating to welfare and safeguarding issues.

Privacy by design

The trust is required to carry out an assessment of the privacy implications of using personal data in certain ways such as when new technology is introduced, where the processing results in a high risk to an individual's privacy or where personal data is used on a large scale.

These assessments referred to as data protection impact assessments are required to identify the measures needed to prevent information security breaches from taking place.

Where there is a need to share personal data with a third party, due diligence must be carried out and reasonable steps taken to ensure that all personal data is adequately protected.

Accuracy and relevance

It is the responsibility of those who receive personal information to make sure so far as is possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate and up to date. If the information is found to be inaccurate, steps must be taken to put it right. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

'Data subjects' have a right to access personal information held about them and have errors corrected.

It is the trust's policy to ensure (where possible) that data processing consent for young people and parental contacts are updated, annually, along with reviewing personal contact information. This should be captured using the trust's standard consent form and where possible collected electorally using MyChildAtSchool (MCAS) app by Bromcom.

Retention and disposal of information

The trust holds personal information. The UK Data Protection Act requires that we do not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed securely when it is no longer needed, provided there is no legal or other business reason for holding it.

The trust's information retention schedule must be checked before records are disposed of, to make sure that the prescribed retention period for that type of record is complied with. Alternatively, advice should be sought from the information and data governance team.

Biometric data

Biometric data is personal information about an individual's physical or behavioural characteristics than can be used to identify a person.

Example of biometric data could include:

- fingerprints
- face shapes
- retina pattern
- iris pattern
- hand measurement

As biometric data is personally identifiable information, its processing must comply with the UK Data Protection Act. Under the UK Data Protection Act biometric data is termed special category (sensitive) personal data.

Where biometric data is used within the trust as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), the trust will comply with the requirements of the Protection of Freedoms Act 2012 and written consent will be obtained before any biometric data is taken and first processed and a data protection impact assessment completed and approved.

Parents/carers will be notified before any additional biometric recognition system is put in place or before their child first takes part in it. The trust will get written consent from at least one parent/carer before any biometric data is taken from their child and first processed. A data protection impact assessment will also be undertaken.

Parents/carers and pupils have the right to choose not to use the trust's biometric system. Alternative means of accessing the relevant system will be provided for those pupils. Parents/carers and pupil can object to participation in the biometric recognition system(s), or withdraw consent, at any time and any relevant data already captured will be deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data; we will not process that data irrespective of any consent given by the pupil and/or parent/carer.

Where employees' members or other adults use the biometric system(s), consent will be obtained before they first take part in it, and alternative means of accessing the relevant service will be provided if they object. Employees and other adults can also withdraw consent at any time, and any relevant data already captured will be deleted.

CCTV and body cameras

Where and whenever CCTV is used around any trust locations to ensure the safety and security of sites, the safety of young people, they will adhere to the CCTV policy, published on the trusts website for the use of these cameras. Full details of the statement of intent for CCTV is outlined in the use of CCTV and surveillance policy.

The trust does not need to ask individuals' permission to use CCTV but will make it clear where individuals are being recorded, and in some cases where audio recording is used for specific cases. Any security cameras will always be clearly visible and there will be prominent signs explaining that CCTV is in use.

Photographs and video

As part of trust activities, photographs are taken and images recorded (video) of individuals for a range of purposes from marketing and promotional purposes, internal display, and to evidence of academic knowledge and progress.

We will obtain written consent from parents/carers, or young people aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the young person. Where we don't need parental consent, we will clearly explain to the young person, and the parent/carer if the young person is under the age of 12 how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other young people are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or young people where appropriate) have agreed to this.

Where the trust takes photographs and videos, uses may include:

- Within academies on notice boards and in prospectuses, brochures, newsletters, etc.
- Outside of trust by external agencies such as the trust appointed photographers, newspapers, campaigns
- Online on our trust/academies website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. If you withdraw consent after photography/video has been published, it may not be possible for us to remove this from all sources.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Devices for taking photographs and video

Employees are to ensure that, only trust owned devices (e.g. cameras and portable devices) are used to take photographs, no personal devices of employees should be used to take photographs of young people.

Unless the photographs are being taken on behalf of the trust by a trust appointed professional photographer/videographer or by the press/media. An employee personal device may be used in exceptional circumstances, if written consent is given by the trust's data protection lead and the designated safeguarding lead.

Photographs and videos should be transferred to trust IT systems (e.g. SharePoint) at the earliest opportunity, and the original files deleted from the device.

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Employees, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Microsoft Copilot. The trust recognises that AI has many uses to help pupils learn but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the trust will treat this as a data breach and will follow the data incidents and breaches process.

Please refer to the trusts use of artificial intelligence (AI) policy.

Training

All employees and governors/trustees' complete data protection and cyber awareness training through their induction programme, this is also an annual refresher requirement for all.

The trust will communicate any changes to policy and legislation where appropriate and ensure that data protection is a core element when considering professional development.

Requests for personal data (subject access requests)

This section outlines how the Learning Community Trust manages Subject Access Requests (SARs) in accordance with the UK GDPR, the UK Data Protection Act 2018, and the Data (Use and Access) Act 2025.

One of the most commonly exercised rights is the right to make a subject access request (SAR). Under this right people are entitled to request a copy of the personal data which the trust holds about them (or in some cases their child) and to certain supplemental information.

Individuals have the right to access their personal data and supplementary information, unless a legal exemption applies. Although under article 15(1A) of UK GDPR (as amended by DUAA), we are required to conduct only **reasonable and proportionate** searches to locate relevant personal data.

Employees must never respond to a subject access request themselves without consulting the digital, IT and data services team, who will liaise with the data protection officer.

Subject access requests do not have to be labelled as such and do not even have to mention data protection. **The trust, where possible requires a data subject to request a subject access request through their online subject access request form.**

Although subject access requests can be requested in other ways; for example, an email which simply states "Please send me copies of my child's attendance" or made verbally are valid subject access requests. The digital, IT and data services team must be informed if a request is received as outlined in the subject access request process who will liaise with the data protection officer for advice on the response. Where requests are vague with no timeframe windows of information are given

through the original request, it is likely that, digital, IT and data services will contact the requestor to clarify this to enable the request to be fulfilled.

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. Children's rights under the GDPR is explained in more detail.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents who have parental responsibility or legally appointed carers of pupils at primary academies may be granted without the express permission of the pupil. This is not a rule and an individual's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above with capacity are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or legally appointed carers of pupils at an academy will not be granted without obtaining the views of the pupil. This is not a rule and an individual's ability to understand their rights will always be judged on a case-by-case basis.

When a subject access request is made, the trust is required to disclose all the requesters personal data which falls within the scope of their request unless a legal exemption applies.

The trust has one calendar month in which to respond to a subject access request, provided the applicant has clearly stated the nature of their request and suitable proof of identification has been supplied. An extension of up to a further 2 months will be applied where a request is deemed complex, or larger data volumes to review.

A month starts on the day the organisation receives the request, even if that day is a weekend or public holiday. The time limit should be calculated from the day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

For example:

- receives a request on 3 September. The time limit will start from the same day. This gives the trust until 3 October to comply with the request.
- if this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.
- if the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.
- this means that the exact number of days to comply with a request varies, depending on the month in which the request was made.

However, information should not be disclosed if it, although this list is not exhaustive;

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- would include another person's personal data that cannot reasonably be anonymised, the other person has not provided consent, and it would be unreasonable to proceed without it
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- is a request that is unfounded or excessive, the trust may refuse to act on it, or charge a reasonable fee to cover administrative costs. The trust will take into account whether the request is repetitive in nature when making this decision
- where any other exemption under the act applies
- when a request is refused, the individual will be told why, and informed that they have the right to complain through the trust's complaints policy in the first instance, and if they are not stratified with the outcome of their complete they can complaint directly to the Information

Commissioners Office.

Data incidents and breaches

The trust understands the importance of keeping personal data secure and will make all reasonable endeavours to ensure that there are no personal data breaches. This is essential for maintaining the trust and confidence of employees, young people, trustees/governors and their parents/carers when the trust uses their information. In the unlikely event of a suspected data breach, the trust will follow the procedure set out in this policy.

Whilst a data breach can be the result of an innocent mistake, real damage is possible if unauthorised access is gained to personal data which could be used by malicious criminals for example cyber-attacks.

All employees will receive awareness training on how to recognise a data breach as part of their data protection training and the trusts policies also contains further information.

The trust is required to report certain breaches to the Information Commissioner's Office (ICO) and to affected data subjects under the UK General Data Protection Regulation (GDPR). There are strict timescales for reporting breaches (within 72 hours of the trust becoming aware of the breach). The trust also has responsibilities to report certain incidents to other regulators such as the Department of Education. The decision as to whether to report a breach to the ICO will be made by the trust on the advice of the data protection officer.

Data breach definition

A data breach is a breach of security which leads to any of the following;

- the loss of personal data
- the accidental or unlawful destruction of personal data
- the disclosure of personal data to an unauthorised third party
- the unlawful or accidental alteration of personal data
- unauthorised access to personal data

Personal data is information;

- from which a person can be identified (either from the information itself or when combined with other information likely to be used to identify the person)

and

- which relates to that person

If employees are in any doubt as to whether an incident constitutes a data breach they must speak to information and data governance team immediately, who will liaise with the data protection officer. This should follow the trust's serious incidents escalations process.

Immediate action and response

On discovering that there has been or there may have been a data breach/infringement you must notify the trusts information and data governance team immediately who will liaise with the data protection officer. Employees are advised to complete the data breach notification form on the staff portal, to report a data breach, although, if it is felt the breach is serious, please contact the team by phone first – then follow up with the completed form.

Once the initial details are gathered, information and data governance team with the data protection officer will consider whether personal data has been accidently or unlawfully;

- lost
- stolen
- destroyed
- altered
- disclosed or made available where it should not have been
- made available to unauthorised people

Trust information and data governance team, with the data protection officer will make an initial assessment of the information contained in the incident report.

The data protection officer will assess whether the breach may need to be reported to the Information Commissioners Office and the individuals affected. The data protection officer will notify the ICO, after approval from the data controller, or trust executive team, when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals. This will be done without undue delay and where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of working days and term time. If the trust is unsure of whether to report a breach, the assumption should be to report it. Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

It will be important to;

- identify what personal data is at risk
- take measures to prevent the breach from worsening e.g. changing password/access codes, removing/deleting an email from inboxes which was sent by mistake
- recover any of the compromised personal data e.g. use back-ups to restore data
- consider whether any outside agencies need to be informed as a matter of urgency e.g. the police in the event of a burglary or Children's Services where the breach may lead to serious harm
- consider whether any affected individuals shall be told about the breach straight away. For example, so that they may take action to protect themselves or because they would find out about the breach from another source. Please note this is different to the mandatory notification to individuals which does not need to be an immediate notification.

Where the ICO must be notified, the data protection officer will do this in accordance with the ICO guidance, via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the awareness of the breach.

As required, the data protection officer will set out:

- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned
- the contact details of data protection officer
- a description of the likely consequences of the personal data breach

If all the above details are not known, the data protection officer will report as much as they can within 72 hours of the awareness of the breach. The report will explain that there is a delay, the reasons why, and when the data protection expects to have further information. The data protection officer will submit the remaining information as soon as possible.

Depending on the outcome of the assessment and the seriousness of the breach, the data protection officer, with the information and data governance team will recommend to the chief operating officer and other member of trust executive whether or not there is also a need to form an escalation committee, in line with the trust serious incident escalation process.

The data protection officer will document all actions and decisions in case these are challenged at a later date by the ICO or an individual affected by the breach. The details will be entered onto trust data breach/incident register held centrally and will consider and follow up on any recommendations or actions outlined in the response from the ICO relating to reportable breaches, as necessary.

Escalation committee for data breaches

The information and data governance team, with the data protection officer, will consult with the chief operating officer to determine an appropriate level of investigation and response to the data breach. The chief operating officer will identify whether there is a need to establish an escalation committee, and which individuals are needed to form the committee. This will depend on the severity, impact, nature and location of the breach and the potential implications. Representation may be required from

a number of stakeholders and the members of this committee will have certain responsibilities. Below is an outline of the areas that may need to be represented and the responsibilities that will need to be considered:

- **Data protection officer:** The data protection officer will be notified of all breaches and will be the point of advice and guidance for the committee in relation to relevant legislation.

- **Head of IT and Data:** The digital innovator and technical lead, will support the data protection officer, through the investigation process and preparation of action, in addition they will lead on ensuring that the trusts IT infrastructure is secure or invoking the correct IT business continuity process.

- **Relevant senior leader/headteacher/principal where the breach occurred:** The senior leader will support the investigation team with providing information, and logistical arrangements for their campus/department.

- **Relevant director of the area where the breach occurred:** The director will support by ensuring relevant senior leaders are timely completing actions as required.

- **Projects and communications lead:** The project and communications lead, will lead on the public and internal communications regarding the breach. Where appropriate, they will liaise with informing/responding to the media regarding the breach.

- **Trust executive:** To have overall oversight and approval of actions for the data breach. The chief executive officer will liaise with the chair of trustees as appropriate. Any decision to report the data breach to the Department of Education will be taken by the chief executive officer.

Contacting the affected data subjects

The trust is required to report a data breach to the individuals whose data has been compromised where the breach is likely to result in a high risk to the rights and freedoms of individuals.

The duty to tell an individual about a breach does not apply if:

- appropriate technical and organisational measures have been implemented which were applied to the personal data affected by the breach (for example the data has been securely encrypted)
- subsequent measures have been taken which will ensure that any high risk to the rights and freedoms to individuals is no longer likely to materialise
- it would involve disproportionate effort

It may not always be clear which individuals shall be notified, for example, parents/carers may need to be notified rather than their children.

If the trust decides not to notify individuals this decision must be documented, on the breach notification actions form.

If a notification is sent this must be done so without undue delay, with approval of the notification contents by the information and data governance team (who will liaise with the data protection officer) and the trust projects and communications lead. The trust shall work with the ICO in the case of a reportable breach in determining when the most appropriate time is to notify the individuals. Other outside agencies, such as the police, may also have a view regarding the timing of this notification. The data protection officer will act as the trusts contact with the ICO.

The ICO may advise or require the trust to notify individuals. In addition, the ICO has the authority to require a more detailed notification to be given to individuals. The ICO is given these powers under the UK Data Protection Act 2018/UK GDPR.

Content of the notification to individuals

The notification to individuals must include the following as a minimum:

- the name and contact details of who can provide more information
- the name and contact details of the data protection officer
- a description of the likely consequences of the data breach
- a description of the measures taken or proposed to be taken by the trust to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In addition, the trust must consider if any additional information would be helpful to data subjects. For example, instructions on measures which they can take to protect their data now or in the future.

The notification must be drafted in clear language. If directed at pupils the notification shall be age appropriate.

The data protection officer and/or escalation committee shall advise on the most appropriate method of communication for the notification. Factors to consider include the urgency of the notification. For example, it may be appropriate to telephone individuals followed up with an email.

Right to complain (data protection)

The Data Use and Access Act 2025 requires the trust to have a complaints process in place where a data subject can make a complaint to the trust about its processing of their personal data.

Complaints will be dealt with in line with the trust's complaints policy and procedure. Complaints in relation to processing of their personal data will be dealt with by the trust's data controller/data protection lead – if the complaint is in relation the data controller/data protection lead, the chief operating officer will review the complaint.

If following these complaints process the data subject remains dissatisfied, they have the right to refer the matter to the Information Commission. Please note the Information Commission require the data subject to go through the trust's data protection complaint process prior to contacting them with any referral.

Privacy notices

Privacy notice for parents and carers – use of your child's personal data

Introduction

Under UK data protection law, individuals have a right to be informed about how the trust and our academies uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice applies while we believe your child is not capable of understanding and exercising their own data protection rights. Once your child is able to understand their rights over their own personal data (generally considered to be age 12, but this has to be considered on a case-by-case basis), you should instead refer to our privacy notice for young people to see what rights they have over their own personal data.

We, the Learning Community Trust of Grosvenor House, Central Park, Telford TF2 9TW, are the 'data controller' for the purposes of UK data protection law. For academies of the Learning Community Trust, the trust is the data controller and is registered under reference ZA285539 with the Information Commissioner's Office.

The personal data we hold

We hold personal data about young people at our academies to support teaching and learning, to provide pastoral support, to ensure the safety of all young people and to assess how the trust/academy is performing.

Personal data that we may collect, use, store and share (when appropriate) about your child includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests/examinations
- Pupil and curricular records
- Exclusion information
- Attendance information
- Safeguarding information
- Behaviour information both positive and negative behaviours
- Details of any support received, including care packages, plans and support providers
- Information about your child's use of our information and communications systems, equipment and facilities (e.g. school computers)

We may also collect, use, store and share (when appropriate) information about your child that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about any medical conditions we need to be aware of, including physical and mental health
- Photographs and CCTV images captured in the academy
- Information about characteristics, such as ethnic background or special educational needs and disabilities (SEND)
- Safeguarding information

We may also hold data about your child that we have received from other organisations, including other schools and local authorities.

Why we use this data

We collect and use the data listed above to:

a. Support young person learning
b. Monitor and report on young people's progress
c. Provide appropriate pastoral support

d. Protect young person welfare
e. Assess the quality of our services
f. Administer admissions
g. Carry out research
h. Administer trust property
i. Comply with the law regarding data sharing
j. Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely

We will only use your young person's personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for any other reason and that reason is incompatible with the original purpose. If we need to use your young person's personal information for an unrelated purpose, we will notify you and explain the legal basis that allows us to do so.

Please note that we may process your young person's personal information without your knowledge or consent in compliance with the above rules where this is required or permitted by law.

Use of your young person's personal data for marketing purposes
Where you have given, us consent to do so, we may send your young person marketing information by email or text promoting academy events, campaigns, charitable causes or services that may be of interest to them.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us to update your young person's marketing consent options.

Use of your young persons' personal data in automated decision-making and profiling
We do not currently process any pupils' personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Use of your young person's personal data for filtering and monitoring purposes
We monitor the use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use agreement) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your young person's welfare

Our lawful basis for using this data

Our lawful bases for processing your young person's personal data for the purposes listed in the why we use this data section above are as follows, as outlined under article 6:

- For the purposes of monitor and report of young person progress, protect young person's welfare, comply with the law regarding data sharing, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school as set out here:
    - Education Act 1996
    - Academies Act 2010
    - Children Act 1989 and 2004
- For the purposes of assessing the quality of our services, administer admissions, administer trust property, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law as set out here:
    - Education (Pupil Registration) Regulations 2006
    - Health and Safety at Work Act 1974
    - Equality Act 2010
- For the purposes of protect young person's welfare in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

Where you have provided us with consent to use your young person's data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law as outlined under article 9:

- We have obtained your explicit consent to use your young person's personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional, or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include as online under article 10:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your young person's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

We will only collect and use your young person's information when the law allows us to as detailed above in our lawful basis for using this data section of this notice. While the majority of information we collect about your young person is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about your young person will come from you, but we may also hold data about your young person from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals
- Other schools or trusts
- Department for Education

How we store this data

We keep personal information about your young person while they are attending our academies. We may also keep it beyond their attendance within our trust if this is necessary to comply with our legal obligations or to meet our regulatory requirements. Our information retention policy sets out how long we keep information about young people. For further information about our information retention policy please contact the trust's digital, IT and data services team by visiting https://portal.lct.education/data-protection/contact.

We have put in place appropriate security measures to prevent your young person's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your young person's personal data securely when we no longer have a legal requirement to retain it.

Who we share data with

We do not share information about your young person with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Schools and educational establishment that your young person may attend after leaving us
- Relevant local authority for the academy young person attends, Telford and Wrekin Council or Shropshire County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions. Other local authorities may be valid were looked after children are in the care of a local authority outside the trust's demographic area
- Government departments or agencies
- Youth support services provider
- Department for Education
- Our regulator, Ofsted
- Awarding bodies for qualifications
- Suppliers and service providers:
    - Alternative provision providers
    - Financial organisations
    - Safeguarding records management organisations
    - Management information systems supply organisations
    - Trust appointed auditors
    - Trust appointed legal partners/solicitors
    - Health authorities
    - Security organisations
    - Health and social welfare organisations
    - Professional advisers and consultants
    - Police forces, courts, tribunals
    - IT management organisations
    - Filtering and monitoring support organisations

Sharing data with the Department for Education (DfE)
The Department for Education (a government department) collects personal data from academies and local authorities via various statutory data collections. We are required to share information about our young people with the DfE either directly or via our local authority, via various statutory data collections.

The data shared will be in line with the following relevant legislation:

- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

The data is transferred securely and held by the Department for Education under a combination of software and hardware controls that meet the current government security policy framework.

The data we share with the DfE is used for a number of purposes, including to:

- Inform funding
- Monitor education policy and academy/trust accountability
- Support research

The information shared with the DfE could include:

- Your young person's name and address
- Unique pupil numbers
- Pupil matching reference numbers
- Gender or ethnicity
- Details of any special educational needs (SEN)
- Details of schools attended
- Absence and exclusion information
- Information relating to exam results
- Information relating to any contact with children's services
- What they did after they finished school

Please note: this list is not exhaustive.

Once your young person reaches the age of 13, we are legally required to pass on certain information to the local authority or youth services provider, which has responsibilities regarding the education or training of 13- to 19-year-olds under section 507B of the Education Act 1996.

Parents/carers, or young people if aged 16 or over, can request that only their name, address and date of birth be passed to these agencies by informing the trust's digital, IT and data service team by visiting https://portal.lct.education/data-protection/.

National Pupil Database (NPD)
We are required to provide information about young people to the DfE as part of statutory data collections such as the school census and early years census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the DfE and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The DfE may share information from the NPD with third parties, such as other organisations that promote children's education or wellbeing in England. These third parties must agree to strict terms and conditions about how they will use the data.

For more information, see the DfE's webpage on how it collects and shares personal data. You can also contact the Department for Education with any further questions about the NPD.

Where we transfer your young person's personal data to a third-party country or territory, we will do so in accordance with UK data protection law. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about your child
You have a right to make a 'subject access request' to gain access to personal information that we hold about your young person.

If you make a subject access request, and if we do hold information about your child, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for

- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your child's personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please see the subject access request section of the trust's data protection policy or by visiting https://portal.lct.education/data-protection.

Once your young person is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), we will need to obtain consent from your young person for you to make a subject access request on their behalf.

Your right to access your child's educational record

Due to young people being at an academy (not a maintained school) there's no automatic parental right of access to the educational record in academies. Therefore, parents would need to submit a subject access request with a detailed list of information requested. For further information please see the subject access request section of the trust's data protection policy.

Your other rights regarding young person's data

Under UK data protection law, you have certain rights regarding how your young person's personal data is used and kept safe. For example, you have the right to:

- Object to our use of your young person's personal data
- Object to the processing of your young person's personal data that is likely to cause, or is causing, damage or distress
- Prevent your young person's data being used to send direct marketing
- Object to and challenge the use of your young person's personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your young person's deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your young person's personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in our lawful basis for using this data section of this privacy notice.

To exercise any of these rights, please contact our digital, IT and data services team by visiting the data protection section of the trust's website.

Once your young person is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), we will need to obtain consent from your young person for you to make a subject access request on their behalf.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us by following the trust's complaints policy, further details are outlined in the complaints section of the trust's data protection policy.

Contact us

If you have any questions or concerns or would like more information about anything mentioned in this privacy notice, please contact our digital, IT and data services team, through the trust's website.

However, our data protection lead has day-to-day responsibility for data protection issues throughout the trust who is the trust's Head of IT and Data. Full details of our data control, data protection lead and data protection officer can be found in the trust's data protection policy.

Privacy notice for young people – use of your personal data

Introduction

Under UK data protection law, individuals have a right to be informed about how the trust and our academies uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about young people throughout the trust, like you.

We, the Learning Community Trust of Grosvenor House, Central Park, Telford TF2 9TW, are the 'data controller' for the purposes of UK data protection law. For academies of the Learning Community Trust, the trust is the data controller and is registered under reference ZA285539 with the Information Commissioner's Office.

The personal data we hold

We hold personal data about you to support teaching and learning, to provide pastoral support, to ensure the safety of all young people and to assess how the trust/academy is performing.

For the same reasons, we get information about you from some other places too – such as other schools, the local council and the government.

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests/examinations
- Pupil and curricular records
- Exclusion information
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Information about your child's use of our information and communications systems, equipment and facilities (e.g. school computers)

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about any medical conditions we need to be aware of, including physical and mental health
- Photographs and CCTV images captured in the academy
- Information about characteristics, such as ethnic background or special educational needs and disabilities (SEND)

We may also hold data about you that we have received from other organisations, including other schools and local authorities.

Why we use this data

We collect and use the data listed above to:

a. Support your learning
b. Monitor and report on your progress
c. Provide appropriate pastoral support
d. Protect your welfare
e. Assess the quality of our services
f. Administer admissions
g. Carry out research
h. Administer trust property
i. Comply with the law regarding data sharing

j. Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely
k. Enable us to contact you/your parents

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for any other reason and that reason is incompatible with the original purpose. If we need to use your young person's personal information for an unrelated purpose, we will notify you and explain the legal basis that allows us to do so.

Please note that we may process your personal information without your knowledge or consent in compliance with the above rules where this is required or permitted by law.

Use of your young person's personal data for marketing purposes
Where you have given, us consent to do so, we may send your young person marketing information by email or text promoting academy events, campaigns, charitable causes or services that may be of interest to them.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us to update your young person's marketing consent options.

Use of your young persons' personal data in automated decision-making and profiling
We do not currently process any pupils' personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Use of your young person's personal data for filtering and monitoring purposes
We monitor the use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use agreement) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your young person's welfare

Our lawful basis for using this data

Our lawful bases for processing your young person's personal data for the purposes listed in the why we use this data section above are as follows:

- For the purposes of monitor and report of young person progress, protect young persons welfare, comply with the law regarding data sharing, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school as set out here:
    - Education Act 1996
    - Academies Act 2010
    - Children Act 1989 and 2004
- For the purposes of assessing the quality of our services, administer admissions, administer trust property, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law as set out here:
    - Education (Pupil Registration) Regulations 2006
    - Health and Safety at Work Act 1974
    - Equality Act 2010
- For the purposes of protect young person's welfare in accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

Where you have provided us with consent to use your young person's data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you will go about withdrawing consent if you wish to do so.

Our basis for using special category data

For ‘special category’ data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your young person’s personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual’s vital interests (i.e. protect your child’s life or someone else’s life), in situations where you’re physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional, or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual’s vital interests (i.e. protect your young persons life or someone else’s life), in situations where you’re physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

We will only collect and use your young person’s information when the law allows us to as detailed above in our lawful basis for using this data section of this notice. While the majority of information we collect about your young person is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about your young person will come from you, but we may also hold data about your young person from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals
- Other schools or trusts
- Department for Education

How we store this data

We keep personal information about your young person while they are attending our academies. We may also keep it beyond their attendance within our trust if this is necessary to comply with our legal obligations or to meet our regulatory requirements. Our information retention policy sets out how long we keep information about young people. For further information about our information retention policy please contact the trust’s digital, IT and data services team by visiting the trust’s website.

We have put in place appropriate security measures to prevent your young person’s personal information from being accidentally lost, used or accessed in an unauthorised way, altered or

disclosed. We will dispose of your young person's personal data securely when we no longer have a legal requirement to retain it.

Who we share data with

We do not share information about your young person with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Schools and educational establishment that your young person may attend after leaving us
- Relevant local authority for the academy young person attends, Telford and Wrekin Council or Shropshire County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions. Other local authorities may be valid were looked after children are in the care of a local authority outside the trust's demographic area
- Government departments or agencies
- Youth support services provider
- Department for Education
- Our regulator, Ofsted
- Awarding bodies for qualifications
- Suppliers and service providers:
    - Alternative provision providers
    - Financial organisations
    - Safeguarding records management organisations
    - Management information systems supply organisations
    - Trust appointed auditors
    - Trust appointed legal partners/solicitors
    - Health authorities
    - Security organisations
    - Health and social welfare organisations
    - Professional advisers and consultants
    - Police forces, courts, tribunals
    - IT management organisations
    - Filtering and monitoring support organisations

Sharing data with the Department for Education (DfE)
The Department for Education (a government department) collects personal data from academies and local authorities via various statutory data collections. We are required to share information about our young people with the DfE either directly or via our local authority, via various statutory data collections.

The data shared will be in line with the following relevant legislation:

- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

The data is transferred securely and held by the Department for Education under a combination of software and hardware controls that meet the current government security policy framework.

The data we share with the DfE is used for a number of purposes, including to:

- Inform funding
- Monitor education policy and academy/trust accountability
- Support research

The information shared with the DfE could include:

- Your young person's name and address
- Unique pupil numbers
- Pupil matching reference numbers

- Gender or ethnicity
- Details of any special educational needs (SEN)
- Details of schools attended
- Absence and exclusion information
- Information relating to exam results
- Information relating to any contact with children's services
- What they did after they finished school

Please note: this list is not exhaustive.

Once you're young person's reaches the age of 13, we are legally required to pass on certain information to the local authority or youth services provider, which has responsibilities regarding the education or training of 13- to 19-year-olds under section 507B of the Education Act 1996.

Parents/carers, or young people if aged 16 or over, can request that only their name, address and date of birth be passed to these agencies by informing the trust's digital, IT and data service team by visiting the trust's website.

National Pupil Database (NPD)
We are required to provide information about young people to the DfE as part of statutory data collections such as the school census and early years census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the DfE and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The DfE may share information from the NPD with third parties, such as other organisations that promote children's education or wellbeing in England. These third parties must agree to strict terms and conditions about how they will use the data.

For more information, see the DfE's webpage on how it collects and shares personal data. You can also contact the Department for Education with any further questions about the NPD.

Where we transfer your young person's personal data to a third-party country or territory, we will do so in accordance with UK data protection law. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about your child
You have a right to make a 'subject access request' to gain access to personal information that we hold about your young person.

If you make a subject access request, and if we do hold information about your child, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your child's personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please see the subject access request section of the trust's data protection policy or by visiting trust's website.

Once your young person is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), we will need to obtain consent from your young person for you to make a subject access request on their behalf.

Your right to access your child's educational record
Due to young people being at an academy (not a maintained school) there's no automatic parental right of access to the educational record in academies. Therefore, parents would need to submit a subject access request with a detailed list of information requested. For further information please see the subject access request section of the trust's data protection policy.

Your other rights regarding young person's data
Under UK data protection law, you have certain rights regarding how your young person's personal data is used and kept safe. For example, you have the right to:

- Object to our use of your young person's personal data
- Object to the processing of your young person's personal data that is likely to cause, or is causing, damage or distress
- Prevent your young person's data being used to send direct marketing
- Object to and challenge the use of your young person's personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your young person's deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your young person's personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in our lawful basis for using this data section of this privacy notice.

To exercise any of these rights, please contact our digital, IT and data services team by visiting the trust's website.

Once your young person is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), we will need to obtain consent from your young person for you to make a subject access request on their behalf.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us by following the trust's complaints policy, further details are outlined in the complaints section of the trust's data protection policy.

Contact us

If you have any questions or concerns or would like more information about anything mentioned in this privacy notice, please contact our digital, IT and data services team, through the trust's website.

However, our data protection lead has day-to-day responsibility for data protection issues throughout the trust who is the trust's Head of IT and Data. Full details of our data control, data protection lead and data protection officer can be found in the trust's data protection policy.

Privacy notice for trust and academy workforce

Introduction

Under UK data protection law, individuals have a right to be informed about how the trust and our academies uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or who otherwise engage to work within our trust. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy as soon as reasonably practical.

We, the Learning Community Trust of Grosvenor House, Central Park, Telford TF2 9TW, are the 'data controller' for the purposes of UK data protection law. For academies of the Learning Community Trust, the trust is the data controller and is registered under reference ZA285539 with the Information Commissioner's Office.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Your name
- Contact details
- Date of birth, marital status, equality, diversity and inclusion information
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in application forms etc
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Information through any investigations or personnel processes

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about any health conditions you have that we need to be aware of, including any occupational health reports and referrals
- Sickness records
- Photographs and CCTV images captured within the trust
- Information about trade union membership
- Safeguarding records as outlined in Keeping Children Safe in Education, and other statutory documents in relation to allegations and low-level concerns

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and local authorities, and the Disclosure and Barring Service in respect of criminal offence data.

Why we use this data

We collect and use the data listed above to:

a. Enable you to be paid
b. Check your entitlement to work in the UK

c. Determine the terms on which you work for us
d. Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
e. Support effective performance management
f. Inform our recruitment and retention policies
g. Allow better financial modelling and planning
h. Enable equalities monitoring
i. Improve the management of workforce data across the sector
j. Support the work of the School Teachers' Review Body
k. Make sure our information and communications systems, equipment and facilities (e.g. computers) are used appropriately, legally and safely
l. Ascertain your fitness to work
m. Manage sickness absence
n. Promote the trust, celebrate success and deal with crisis management
o. Protect your wellbeing and safety

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Use of your personal data for marketing purposes
Where you have given, us consent to do so, we may send your young person marketing information by email or text promoting academy events, campaigns, charitable causes or services that may be of interest to them.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us to update your marketing consent options.

Use of your personal data in automated decision-making and profiling
We do not currently process any personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Use of your young person's personal data for filtering and monitoring purposes
We monitor the use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use agreement) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your and our young people's welfare

Our lawful basis for using this data

Our lawful bases for processing your young person's personal data for the purposes listed in the why we use this data section above are as follows:

- For the purposes of b, d, h, i, j in accordance with the 'public task' basis.
- For the purposes of a, b, c, d, f, h, l, in accordance with the 'legal obligation' basis.
- For the purposes of n, in accordance with the 'consent' basis – we will obtain consent from you to use your personal data

- For the purposes of k, o, accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

Where you have provided us with consent to use your personal data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

We will only collect and use your data when the law allows us to as detailed above in our lawful basis for using this data section of this notice. While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Adapt the list below to reflect the sources of any data you've obtained from anyone other than the individual.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals
- Pervious employers

How we store this data

We keep personal information about your young person while they are attending our academies. We may also keep it beyond their attendance within our trust if this is necessary to comply with our legal

obligations or to meet our regulatory requirements. Our information retention policy sets out how long we keep information about young people. For further information about our information retention policy please contact the trust's digital, IT and data services team by visiting the trust's website.

We have put in place appropriate security measures to prevent your young person's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your young person's personal data securely when we no longer have a legal requirement to retain it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Relevant local authority for the academy young person attends, Telford and Wrekin Council or Shropshire County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns.
- Government departments or agencies
- Department for Education
- Our regulator, Ofsted, Teachers Regulation Authority etc
- Suppliers and service providers:
    - Financial organisations
    - Payroll management organisations
    - Human resources management organisations
    - Safeguarding records management organisations
    - Management information systems supply organisations
    - Personal development system supply and support organisations
    - Trust appointed auditors
    - Trust appointed legal partners/solicitors
    - Health authorities
    - Security organisations
    - Health and social welfare organisations
    - Professional advisers and consultants
    - Police forces, courts, tribunals
    - IT management organisations
    - Filtering and monitoring support organisations

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please see the subject access request section of the trust's data protection policy or by visiting the trust's website.

Your other rights regarding your person's data
Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Object to the processing of your personal data that is likely to cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in our lawful basis for using this data section of this privacy notice.

To exercise any of these rights, please contact our digital, IT and data services team by visiting the trust's website.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us by following the trust's complaints policy, further details are outlined in the complaints section of the trust's data protection policy.

Contact us

If you have any questions or concerns or would like more information about anything mentioned in this privacy notice, please contact our digital, IT and data services team, through the trust's website.

However, our data protection lead has day-to-day responsibility for data protection issues throughout the trust who is the trust's Head of IT and Data. Full details of our data control, data protection lead and data protection officer can be found in the trust's data protection policy.

Privacy notice for governors, trustees and other volunteers

Introduction

Under UK data protection law, individuals have a right to be informed about how the trust and our academies uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals working with the trust in a voluntary capacity, including governors/trustee.

We, the Learning Community Trust of Grosvenor House, Central Park, Telford TF2 9TW, are the 'data controller' for the purposes of UK data protection law. For academies of the Learning Community Trust, the trust is the data controller and is registered under reference ZA285539 with the Information Commissioner's Office.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Your name
- Contact details
- Date of birth, and equality diversity and inclusion monitoring information
- Next of kin and emergency contact numbers
- Recruitment information, including references and other information included in application forms etc
- Information about business and pecuniary interests
- Information through any investigations or personnel processes

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about any health conditions you have that we need to be aware of
- Information about disability and access requirements
- Photographs and CCTV images captured within the trust
- Safeguarding records as outlined in Keeping Children Safe in Education, and other statutory documents in relation to allegations and low-level concerns

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and local authorities, and the Disclosure and Barring Service in respect of criminal offence data.

Why we use this data

We collect and use the data listed above to:

a. Establish and maintain effective governance
b. Meet statutory obligations for publishing and sharing governors'/trustees' details
c. Facilitate safe recruitment, as part of our safeguarding obligations
d. Undertake equalities monitoring
e. Ensure that appropriate access arrangements can be provided for volunteers who require them
f. Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely
g. Promote the trust, celebrate success and detail with
h. Promote the trust, celebrate success and deal with crisis management
i. Protect your wellbeing and safety

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers and young people).

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Use of your personal data for marketing purposes
Where you have given, us consent to do so, we may send your young person marketing information by email or text promoting academy events, campaigns, charitable causes or services that may be of interest to them.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us to update your marketing consent options.

Use of your personal data in automated decision-making and profiling
We do not currently process any personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Use of your personal data for filtering and monitoring purposes
We monitor the use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use agreement) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your and our young people's welfare

Our lawful basis for using this data

Our lawful bases for processing your young person's personal data for the purposes listed in the why we use this data section above are as follows:

- For the purposes of a, b, c, in accordance with the 'public task' basis.
- For the purposes of a, b, c, d, e, f in accordance with the 'legal obligation' basis.
- For the purposes of g, in accordance with the 'consent' basis – we will obtain consent from you to use your personal data
- For the purposes of f, h, accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

Where you have provided us with consent to use your personal data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent

- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

We will only collect and use your data when the law allows us to as detailed above in our lawful basis for using this data section of this notice. While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Adapt the list below to reflect the sources of any data you've obtained from anyone other than the individual.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals
- Pervious employers

How we store this data

We keep personal information about your young person while they are attending our academies. We may also keep it beyond their attendance within our trust if this is necessary to comply with our legal obligations or to meet our regulatory requirements. Our information retention policy sets out how long we keep information about young people. For further information about our information retention policy please contact the trust's digital, IT and data services team by visiting the trust's website..

We have put in place appropriate security measures to prevent your young person's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your young person's personal data securely when we no longer have a legal requirement to retain it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Relevant local authority for the academy young person attends, Telford and Wrekin Council or Shropshire County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns.
- Government departments or agencies
- Department for Education
- Our regulator, Ofsted, Teachers Regulation Authority etc
- Suppliers and service providers:
    - Financial organisations
    - Safeguarding records management organisations
    - Management information systems supply organisations
    - Personal development system supply and support organisations
    - Trust appointed auditors
    - Trust appointed legal partners/solicitors
    - Health authorities
    - Security organisations
    - Health and social welfare organisations
    - Professional advisers and consultants
    - Police forces, courts, tribunals
    - IT management organisations
    - Filtering and monitoring support organisations

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please see the subject access request section of the trust's data protection policy or by visiting https://portal.lct.education/data-protection.

Your other rights regarding your person's data
Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Object to the processing of your personal data that is likely to cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)

- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in our lawful basis for using this data section of this privacy notice.

To exercise any of these rights, please contact our digital, IT and data services team by visiting the trust's website.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us by following the trust's complaints policy, further details are outlined in the complaints section of the trust's data protection policy.

Contact us

If you have any questions or concerns or would like more information about anything mentioned in this privacy notice, please contact our digital, IT and data services team, through the trust's website.

However, our data protection lead has day-to-day responsibility for data protection issues throughout the trust who is the trust's Head of IT and Data. Full details of our data control, data protection lead and data protection officer can be found in the trust's data protection policy.

Privacy notice for visitors

Introduction

Under UK data protection law, individuals have a right to be informed about how the trust and our academies uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals who are visitors to our academies and the trust.

We, the Learning Community Trust of Grosvenor House, Central Park, Telford TF2 9TW, are the 'data controller' for the purposes of UK data protection law. For academies of the Learning Community Trust, the trust is the data controller and is registered under reference ZA285539 with the Information Commissioner's Office.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Your name
- Contact details
- Information relating to your visit, eg. company or organisation, arrival and departure time, vehicle number plate

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about disability and access requirements
- Photographs and CCTV images captured within the trust
- Safeguarding records as outlined in Keeping Children Safe in Education, and other statutory documents in relation to allegations and low-level concerns

We may also hold data about you that we have received from other organisations, including other schools and local authorities.

Why we use this data

We collect and use the data listed above to:

a. Identify you and keep you safe while on our campuses
b. Keep young people, workforce and volunteers safe
c. Maintain accurate records of visits to the trust
d. Provide appropriate access arrangements
e. Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely
f. Meet legal requirements placed upon us
g. Promote the trust, celebrate success and deal with crisis management
h. Protect your wellbeing and safety

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Use of your personal data for marketing purposes
Where you have given, us consent to do so, we may send you marketing information by email or text promoting academy events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us to update your marketing consent options.

Use of your personal data in automated decision-making and profiling
We do not currently process any personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Use of your personal data for filtering and monitoring purposes
We monitor the use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use agreement) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your and our young people's welfare

Our lawful basis for using this data

Our lawful bases for processing your young person's personal data for the purposes listed in the why we use this data section above are as follows:

- For the purposes of c, f, in accordance with the 'public task' basis.
- For the purposes of a, b, c, d, e, f in accordance with the 'legal obligation' basis.
- For the purposes of g, in accordance with the 'consent' basis – we will obtain consent from you to use your personal data
- For the purposes of b, h, accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

Where you have provided us with consent to use your personal data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent

- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

We will only collect and use your data when the law allows us to as detailed above in our lawful basis for using this data section of this notice. While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Adapt the list below to reflect the sources of any data you've obtained from anyone other than the individual.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals
- Other schools or trusts

How we store this data

We keep personal information about you while you are visiting our campuses. We may also keep it beyond your visit to our trust if this is necessary to comply with our legal obligations or to meet our regulatory requirements. Our information retention policy sets out how long we keep information about young people. For further information about our information retention policy please contact the trust's digital, IT and data services team by visiting the trust's website.

We have put in place appropriate security measures to prevent your young person's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your young person's personal data securely when we no longer have a legal requirement to retain it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Relevant local authority for the academy young person attends, Telford and Wrekin Council or Shropshire County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns.
- Government departments or agencies
- Department for Education
- Our regulator, Ofsted
- Suppliers and service providers:
    - Financial organisations
    - Safeguarding records management organisations
    - Management information systems supply organisations
    - Trust appointed auditors
    - Trust appointed legal partners/solicitors
    - Health authorities
    - Security organisations
    - Health and social welfare organisations
    - Professional advisers and consultants

- Police forces, courts, tribunals
- IT management organisations
- Filtering and monitoring support organisations

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please see the subject access request section of the trust's data protection policy or by visiting the trust's website.

Your other rights regarding your person's data
Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Object to the processing of your personal data that is likely to cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in our lawful basis for using this data section of this privacy notice.

To exercise any of these rights, please contact our digital, IT and data services team by visiting the trust's website.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us by following the trust's complaints policy, further details are outlined in the complaints section of the trust's data protection policy.

Contact us

If you have any questions or concerns or would like more information about anything mentioned in this privacy notice, please contact our digital, IT and data services team, through the trust's website.

However, our data protection lead has day-to-day responsibility for data protection issues throughout the trust who is the trust's Head of IT and Data. Full details of our data control, data protection lead and data protection officer can be found in the trust's data protection policy.

Privacy notice for suppliers and customers

Introduction

Under UK data protection law, individuals have a right to be informed about how the trust and our academies uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about suppliers of goods and services that the trust, either directly or through 1 of our academies, contracts with, including their individual representatives, employees and agents. References to "you" in this privacy notice cover all of these individuals.

We, the Learning Community Trust of Grosvenor House, Central Park, Telford TF2 9TW, are the 'data controller' for the purposes of UK data protection law. For academies of the Learning Community Trust, the trust is the data controller and is registered under reference ZA285539 with the Information Commissioner's Office.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Names, characteristics and contact details
- References, CVs and details of an individual's employment history, if collected as part of a bidding, tendering or engagement process
- Bank details and other financial information where it relates to an individual, such as if you're operating as a sole trader
- Any other personal information necessary to fulfil the terms of a contract we have with you
- Information relating to visits to our campuses, e.g. the individual's company or organisation name, arrival and departure time, vehicle number plate
- Information about your use of our information and communication systems, equipment and facilities

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about disability and access requirements
- Photographs and CCTV images captured within the trust
- Safeguarding records as outlined in Keeping Children Safe in Education, and other statutory documents in relation to allegations and low-level concerns

We may also hold data about you that we have received from other organisations, including other schools and local authorities.

Why we use this data

We collect and use the data listed above to:

a. Decide whether to engage you
b. Fulfil the terms of our contract with you, including payment
c. Keep accurate records of the suppliers that we use
d. Identify you while on our campus, and keep all individuals safe
e. Keep pupils and staff safe while you are on the campus
f. Keep accurate records of visits to the campus
g. Make sure our information and communication systems, equipment and facilities (e.g. computers) are used appropriately, legally and safely
h. Meet legal requirements placed upon us

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the

original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Use of your personal data for marketing purposes
Where you have given, us consent to do so, we may send you marketing information by email or text promoting academy events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us to update your marketing consent options.

Use of your personal data in automated decision-making and profiling
We do not currently process any personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Use of your personal data for filtering and monitoring purposes
We monitor the use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use agreement) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your and our young people's welfare

Our lawful basis for using this data

Our lawful bases for processing your young person's personal data for the purposes listed in the why we use this data section above are as follows:

- For the purposes of a, f, h in accordance with the 'public task' basis.
- For the purposes of b, c, d, e, f, g, h, in accordance with the 'legal obligation' basis.
- For the purposes of e, accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

Where you have provided us with consent to use your personal data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

We will only collect and use your data when the law allows us to as detailed above in our lawful basis for using this data section of this notice. While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Adapt the list below to reflect the sources of any data you've obtained from anyone other than the individual.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals

How we store this data

We keep personal information about you while you are a supplier of the trust. We may also keep it beyond your contract with the trust if this is necessary to comply with our legal obligations or to meet our regulatory requirements. Our information retention policy sets out how long we keep information about young people. For further information about our information retention policy please contact the trust's digital, IT and data services team by visiting https://portal.lct.education/data-protection/contact.

We have put in place appropriate security measures to prevent your young person's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your young person's personal data securely when we no longer have a legal requirement to retain it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Relevant local authority for the academy young person attends, Telford and Wrekin Council or Shropshire County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns.
- Government departments or agencies
- Department for Education
- Our regulator, Ofsted
- Suppliers and service providers:
    - Financial organisations

- Safeguarding records management organisations
- Management information systems supply organisations
- Trust appointed auditors
- Trust appointed legal partners/solicitors
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- IT management organisations
- Filtering and monitoring support organisations

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please see the subject access request section of the trust's data protection policy or by visiting the trust's website.

Your other rights regarding your person's data
Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Object to the processing of your personal data that is likely to cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in our lawful basis for using this data section of this privacy notice.

To exercise any of these rights, please contact our digital, IT and data services team by visiting trust's website.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us by following the trust's complaints policy, further details are outlined in the complaints section of the trust's data protection policy.

Contact us

If you have any questions or concerns or would like more information about anything mentioned in this privacy notice, please contact our digital, IT and data services team, through the trust's website.

However, our data protection lead has day-to-day responsibility for data protection issues throughout the trust who is the trust's Head of IT and Data. Full details of our data control, data protection lead and data protection officer can be found in the trust's data protection policy.

Privacy notice for alumni

Introduction

Under UK data protection law, individuals have a right to be informed about how the trust and our academies uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals who are alumni people of our academies.

We, the Learning Community Trust of Grosvenor House, Central Park, Telford TF2 9TW, are the 'data controller' for the purposes of UK data protection law. For academies of the Learning Community Trust, the trust is the data controller and is registered under reference ZA285539 with the Information Commissioner's Office.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name
- Contact details
- Details about your time at the academy, including records of your achievements and interests
- Records of contributions you have made to the trust since leaving
- Records of how you have engaged with our alumni network, including emails you have opened, events attended, mailing lists you have signed up to and any other interaction
- Information about your use of our information and communication systems, equipment and facilities (e.g. computers)

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about disability and access requirements
- Photographs and CCTV images captured within the trust
- Safeguarding records as outlined in Keeping Children Safe in Education, and other statutory documents in relation to allegations and low-level concerns

We may also hold data about you that we have received from other organisations, including other schools and local authorities.

Why we use this data

We collect and use the data listed above to:

a. Help us build a community around the academy/trust
b. Offer enrichment and career development opportunities to current young people
c. Raise extra money so that we can continue to improve the experience
d. Notify you of alumni events you may be interested in
e. Keep you up to date with trust news
f. Help us promote the trust
g. Keep you safe and comfortable while attending alumni events
h. Tailor the communications we send to you, to ensure they are appropriate and relevant
i. Make sure our information and communication systems, equipment and facilities (e.g. computers) are used appropriately, legally and safely
j. Meet legal requirements placed upon us

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Use of your personal data for marketing purposes
Where you have given, us consent to do so, we may send you marketing information by email or text promoting academy events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us to update your marketing consent options.

Use of your personal data in automated decision-making and profiling
We do not currently process any personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Use of your personal data for filtering and monitoring purposes
We monitor the use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use agreement) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your and our young people's welfare

Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed in the why we use this data section above are as follows:

- For the purposes of g, i, j, in accordance with the 'legal obligation' basis.
- For the purposes of g, accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

Where you have provided us with consent to use your personal data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

We will only collect and use your data when the law allows us to as detailed above in our lawful basis for using this data section of this notice. While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Adapt the list below to reflect the sources of any data you've obtained from anyone other than the individual.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals

How we store this data

We keep personal information about you while you are an alumni network. We may also keep it beyond this if the trust deems necessary to comply with our legal obligations or to meet our regulatory requirements. Our information retention policy sets out how long we keep information about young people. For further information about our information retention policy please contact the trust's digital, IT and data services team by visiting the trust's website.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your young person's personal data securely when we no longer have a legal requirement to retain it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Relevant local authority for the academy young person attends, Telford and Wrekin Council or Shropshire County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns.
- Government departments or agencies
- Department for Education
- Our regulator, Ofsted
- Suppliers and service providers:
    - Financial organisations
    - Safeguarding records management organisations
    - Management information systems supply organisations
    - Trust appointed auditors
    - Trust appointed legal partners/solicitors
    - Health authorities
    - Security organisations
    - Health and social welfare organisations

- Professional advisers and consultants
- Police forces, courts, tribunals
- IT management organisations
- Filtering and monitoring support organisations

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please see the subject access request section of the trust's data protection policy or by visiting the trust's website.

Your other rights regarding your person's data
Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Object to the processing of your personal data that is likely to cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests

- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in our lawful basis for using this data section of this privacy notice.

To exercise any of these rights, please contact our digital, IT and data services team by visiting the trust's website.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us by following the trust's complaints policy, further details are outlined in the complaints section of the trust's data protection policy.

Contact us

If you have any questions or concerns or would like more information about anything mentioned in this privacy notice, please contact our digital, IT and data services team, through the trust's website.

However, our data protection lead has day-to-day responsibility for data protection issues throughout the trust who is the trust's Head of IT and Data. Full details of our data control, data protection lead and data protection officer can be found in the trust's data protection policy.

Privacy notice for applications for employment and voluntary positions

Introduction

Under UK data protection law, individuals have a right to be informed about how the trust and our academies uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals who are apply for employment and/or voluntary positions within the trust.

We, the Learning Community Trust of Grosvenor House, Central Park, Telford TF2 9TW, are the 'data controller' for the purposes of UK data protection law. For academies of the Learning Community Trust, the trust is the data controller and is registered under reference ZA285539 with the Information Commissioner's Office.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Your name
- Contact details
- Copies of right to work documentation
- References
- Evidence of qualifications
- Employment records, including work history, job titles, training records and professional memberships
- Information about your use of our information and communication systems, equipment and facilities (e.g. computers)

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about race, ethnicity, religious beliefs, gender identity, sexual orientation and political opinions
- Information about disability and access requirements
- Photographs and CCTV images captured within the trust
- Safeguarding records as outlined in Keeping Children Safe in Education, and other statutory documents in relation to allegations and low-level concerns

We may also hold data about you that we have received from other organisations, including other schools and local authorities, and the Disclosure and Barring Service in respect of criminal offence data.

Why we use this data

We collect and use the data listed above to:

a. Enable us to establish relevant experience and qualifications
b. Facilitate safe recruitment, as part of our safeguarding obligations
c. Enable equalities monitoring
d. Ensure that appropriate access arrangements can be provided for candidates that require them
e. Make sure our information and communication systems, equipment and facilities (e.g. computers) are used appropriately, legally and safely
f. To communicate with applicants about other employment opportunities

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require references for this role and you fail to provide us with the relevant details, we will not be able to take your application further.

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Use of your personal data for marketing purposes
Where you have given, us consent to do so, we may send you marketing information by email or text promoting academy events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by contacting us to update your marketing consent options.

Use of your personal data in automated decision-making and profiling
We do not currently process any personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Use of your personal data for filtering and monitoring purposes
We monitor the use of our information and communication systems, equipment and facilities (e.g. trust computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use agreement) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your and our young people's welfare

Our lawful basis for using this data

Our lawful bases for processing your young person's personal data for the purposes listed in the why we use this data section above are as follows:

- For the purposes of g, i, j, in accordance with the 'legal obligation' basis.
- For the purposes of g, accordance with the 'vital interests' basis – we will use this personal data in a life-or-death situation

Where you have provided us with consent to use your personal data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Collecting this data

We will only collect and use your data when the law allows us to as detailed above in our lawful basis for using this data section of this notice. While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Adapt the list below to reflect the sources of any data you've obtained from anyone other than the individual.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Government departments or agencies
- Police forces, courts or tribunals

How we store this data

We keep personal information about you while you are an alumni network. We may also keep it beyond this if the trust deems necessary to comply with our legal obligations or to meet our regulatory requirements. Our information retention policy sets out how long we keep information about young people. For further information about our information retention policy please contact the trust's digital, IT and data services team by visiting https://portal.lct.education/data-protection/contact.

We have put in place appropriate security measures to prevent your young person's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your young person's personal data securely when we no longer have a legal requirement to retain it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Relevant local authority for the academy young person attends, Telford and Wrekin Council or Shropshire County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns.
- Government departments or agencies
- Department for Education
- Our regulator, Ofsted
- Suppliers and service providers:
    - Financial organisations

- Safeguarding records management organisations
- Management information systems supply organisations
- Trust appointed auditors
- Trust appointed legal partners/solicitors
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- IT management organisations
- Filtering and monitoring support organisations

Where we transfer your personal data to a third-party country or territory, we will do so in accordance with UK data protection law. In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

How to access personal information that we hold about you
You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please see the subject access request section of the trust's data protection policy or by visiting https://portal.lct.education/data-protection.

Your other rights regarding your person's data
Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Object to the processing of your personal data that is likely to cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in our lawful basis for using this data section of this privacy notice.

To exercise any of these rights, please contact our digital, IT and data services team by visiting the trust's website.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us by following the trust's complaints policy, further details are outlined in the complaints section of the trust's data protection policy.

Contact us

If you have any questions or concerns or would like more information about anything mentioned in this privacy notice, please contact our digital, IT and data services team, through the trust's website.

However, our data protection lead has day-to-day responsibility for data protection issues throughout the trust who is the trust's Head of IT and Data. Full details of our data control, data protection lead and data protection officer can be found in the trust's data protection policy.

Standard young person data processing consent from

About the young person

First name
Last name
Pupil date of birth
Academy attending

Photo, video and communications

There are occasions where we capture photographs and videos of our young people to showcase life at our academies. These images and recordings may be used in a variety of communications, including newsletters, the Trust and academy websites, and other promotional materials.
We may also share photographs, names, and achievements through public channels such as social media platforms and local or national media, in order to celebrate the successes of our academies and their students.

Any photos, videos and communications may be used after the young person has left the academy, where consent was given while they were at the academy.

At any time, you can object to our use of this data or withdraw your consent, and we'll stop using your young person's photos or videos, although, it will not be possible to remove all references, but we stop using your information - for this type of data you'll need to do this in writing, so please email the academy revoking consent. You can also contact dataprotection@lct.education to be supported by the trust digital, IT and data services team.

Please tick the relevant boxes below, to agree for consent for the named young person

Ref	Area of consent	Consent granted, please tick
PVC1	**Young person's full name to be used on trust/academy website, printed publications and media whist being at the academy.** Once published information may exist after the young person leaves the academy. This information could be viewed by external parties and potentially worldwide.	
PVC2	**Photos and/or videos of my young person to be taken by the trust/academy.** We require to your consent to take photographs/videos of your young person, which could be used within the academy (eg. academy photos) and as outlined in the other areas of consent on this form.	
PVC3	**Photos and video of my young person to be used in academy and trust newsletters which will be communicated with current parent/carers.** Although this is mainly communicated direct, they will be published on academy websites also. Once published information may exist after the young person leave the academy. This information could be viewed by external parties and potentially worldwide.	
PVC4	**Photos and/or video of my young person to be used on the academy and trust website.** This information could be viewed by external parties and potentially worldwide. Once published information may exist after the young person leave the academy.	

PVC5	**Photos and/or video of my young person to be used as part of media releases (e.g. newspapers, online news outlets etc) and social media channel.** Once published information may exist after the young person leave the academy. It is not always possible to remove images from external companies (e.g. newspapers) once submitted. Therefore, we will always try to remove images if consent is revoked, but cannot guarantee. This information could be viewed by external parties and potentially worldwide.
PVC6	**Photos and/or videos of my young person to be in printed publications (e.g. prospectus, flyers etc).** Once published information may exist after the young person leaves the academy. This information could be viewed by external parties and potentially worldwide.
PVC7	**Photos and/or videos of my young person to be used within the academy (e.g. on school books, internal wall displays etc).** Once published information may exist after the young person leaves the academy.

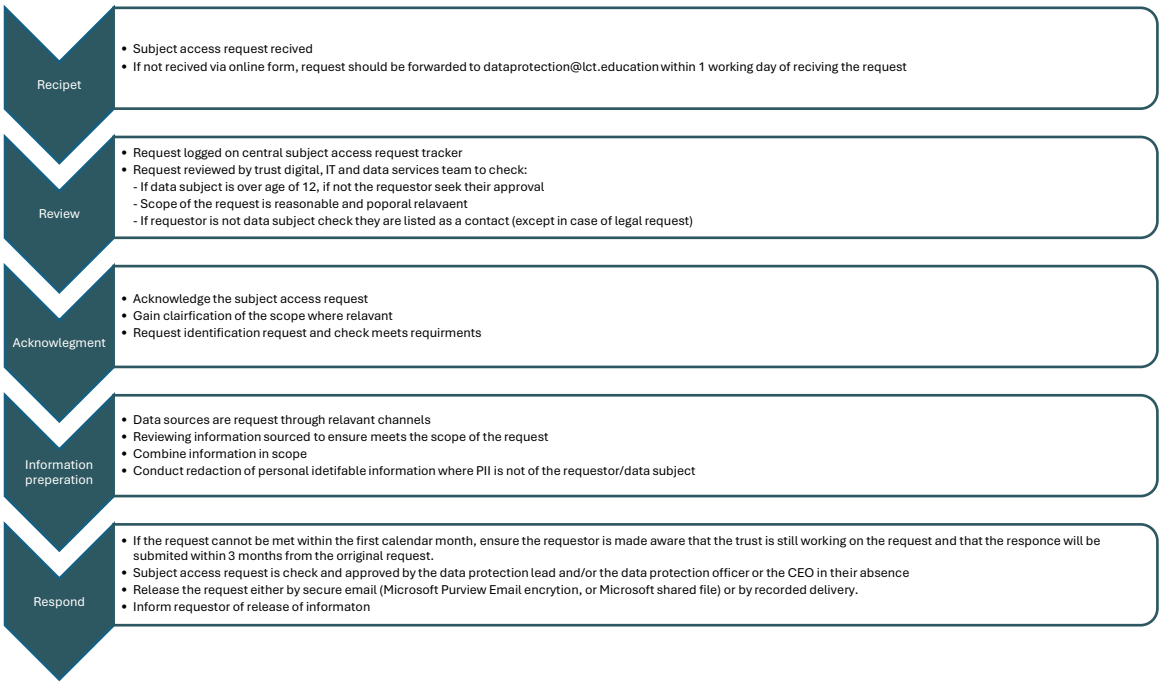
Biometric data (remove if academy does not use biometrics)

We use what is known as 'biometric data' in our academies. Specifically, we use your young person's fingerprints. We'd like your consent to use your young person fingerprints in the ways listed below. This information is held securely in trust systems and helps us operate these systems more efficiently.

At any time, you can object to our use of this data or withdraw your consent, and we'll stop using your young person's fingerprints in the ways described below – for this type of data you'll need to do this in writing, so please email the academy revoking consent. You can also contact dataprotection@lct.education to be supported by the trust digital, IT and data services team.

Ref	Area of consent	Consent granted, please tick
BMD1	**Young person's fingerprint o be used for them to receive school meals.**	
BMD2	**Young persons fingerprint to be used for them to add money to their account.**	

Appendix 4 – Subject access request process



Version control

Version	Date	Updated by	Reason
1	March 2024	Head of Governance and Corporate Support	First issue of trust wide policy.
2	February 2025	Digital Innovator and Technical Lead	Review in line with statutory guidance and trust requirements.
3	November 2025	Head of IT and Data	Including Data Use and Access Act 2025, and structural changes.