Learning Community Trust

Data protection policy

Date	Feb 2025
Version	2
Circulation	Public
Owner	Digital Innovator and Technical Lead
Date approved	13 Feb 2025
Approved by	Audit and Risk Committee
Review date	March 2028
Status	Approved

Contents

Introduction

The UK Data Protection Act 2018/UK GDPR defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Personal information is information about a living individual, who can be identified from the information.

The Learning Community Trust is committed to protecting the privacy of individuals and handles all personal information in a manner that complies with the UK Data Protection Act 2018. It is the personal responsibility of all employees (temporary or permanent), governors, contractors, agents and anyone else processing information on our behalf to comply with this policy.

The board of trustees are ultimately accountable for how personal information is handled and has overall responsibility for ensuring that the trust complies with all relevant data protection obligations. The Digital Innovator and Technical Lead who is the data controller and data protection lead, on a day-to-day basis. In this policy, the term "trust" means both the academy and the central team.

The Learning Community Trust has appointed the information governance service at Telford & Wrekin Council as the trusts data protection officer. The service will support the trust's internal digital, IT and data services team in the development and implementation of data protection policies. The service will support the trust as outlined in the service agreement. The service can be contacted through the trust, by selecting 'data protection' from the contact form options on the trusts website (lct.education).

This policy is applicable to all people working in the trust (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities. Any breach of this policy may result in disciplinary and/or legal action.

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.

GDPR principles

The UK Data Protection Act 2018/UK GDPR 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 2018/UK GDPR 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 2018/UK GDPR. The trust's data protection officer undertakes an annual exercise to ensure that the trust complies with this principle.

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/GDPR 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 Digital Innovator and Technical Lead, 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 contact 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.

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 trusts academies.

Headteacher/principal

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

Employees

Employees are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the trust of any changes to their personal data, such as a change of address
- Contacting the digital, IT and data services 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 or not 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

Individuals' rights

Individuals have a number of rights under the UK Data Protection Act 2018/UK GDPR.

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 digital, IT and data services team as soon as the request is received, as they will liaise with the trust's data protection officer.

Information that falls within scope

The data protection law concerns information about living individuals. Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifier we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Examples of places where personal data might be found are:

- on a computer database
- in a file, such as a pupil report
- a register or contract of employment
- pupils' exercise books, coursework and mark books
- education plans and health records
- email correspondence

Examples of documents where personal data might be found are:

- a report about a child protection incident
- a record about disciplinary action taken against an employee
- photographs/images of pupils
- a recording of a teacher assessment
- contact details and other personal information held about pupils, parents, their families and employees
- contact details of a member of the public who is enquiring about admissions
- information on a pupil's performance
- an opinion about a parent/carer or colleague in an email

The UK Data Protection Act 2018/UK GDPR defines special category personal information as information relating to:

- race and ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- processing of genetic/biometric data to uniquely identifying a person
- physical or mental health or medical condition
- sexual life

Personal data held must be:

Processed fairly, lawfully and transparently

Processing data is any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

When the Learning Community Trust processes personal information, it must have a lawful basis for doing so. The UK Data Protection Act 2018/UK GDPR provides a list of 'conditions' when we can process personal and/or 'special category' personal information.

Individuals must be told what data is collected about them, what it is used for, and who it might be shared with. They must also be given other information, such as, what rights they have in their information, how long it is kept for and about their right to complain to the Information Commissioner's Office (ICO), the data protection regulator. This information is provided in the trust privacy notices and can be obtained from the trust websites.

If personal data is being used in a way that does not comply with data protection law, this should be raised with the digital, IT and data services team, who will liaise with the data protection officer.

Personal data must only be processed for the following purposes:

- to ensure that the trust provides a safe and secure environment
- to provide pastoral care
- to provide education and learning for pupils
- to provide additional activities for pupils and parents/carers (for example activity clubs)
- to protect and promote the trusts interests and objectives (for example fundraising)
- to safeguard and promote the welfare of pupils
- to perform a task in the public interest or in order to carry out official functions as authorised by law
- the processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract

If there is a need to process personal data that is not on the above list, or is not set out in the relevant privacy notice(s), it would be appropriate to contact the digital, IT and data services team to ensure that a lawful reason for using the personal data has been identified.

In some instances, consent may need to be obtained from the individual to use their personal data which must meet certain requirements. In order for consent to be valid it must be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress and should be recorded. Guidance on how consent should be managed can be found from the digital, IT and data services team.

Processed for limited purposes and in an appropriate way

Personal data should only be used for the purposes that it has been collected. For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, the photographs should not be used for another purpose (e.g. a prospectus or social media). Please see child protection and safeguarding policy guidance note relating to the use of images. Trust code of conduct also provides further information relating to the appropriate use of personal data.

Adequate and relevant for the purpose

The trust will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes. Data minimisation will be employed.

Not be excessive or unnecessary

Personal data must not be processed in a way that is excessive or unnecessary. For example, information should only be collected about a pupil's medical history if that personal data has some relevance, such as allowing the trust to care for the pupil and meet their medical needs.

Accurate

The trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the trust.

Not kept for longer than necessary

The UK Data Protection Act 2018/UK GDPR 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 trusts information and data 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 trusts digital, IT and data services team.

Kept secure

All policies and guidance relating to the handling of personal data must be complied with. These include, but are not limited to, IT acceptable use agreement, IT security policy and information security policy.

Not transferred outside the UK/EEA without adequate protection

If personal data needs to be transferred outside the UK/EEA please contact digital, IT and data services, who will liaise with the data protection officer.

The trust should not transfer personal data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK Data Protection Act 2018/UK GDPR. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country. This include signing up to resources and systems.

Sharing personal information

The trust will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. In addition, there must be a legal basis established to share personal data.

The following points will be considered:

- whether the third party has a need to know the information for the purposes of providing the contracted services
- whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained
- whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures
- whether the transfer complies with any applicable cross border transfer restrictions
- whether a fully executed written contract that contains UK Data Protection Act 2018/UK GDPR approved third party clauses has been obtained.

There may be circumstances where the trust is required either by law or in the best interests of our pupils, parents or employees to pass information onto external authorities for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the trust shall be clearly defined within written notifications including details and the basis for sharing the data.

Sharing personal data outside of the trust

- DO share personal data on a "need to know" basis and think about why it is necessary to share data outside of the trust.

- DO encrypt external emails which 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 digital, IT and data services 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 digital, IT and data services. 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 user areas and emails, transfers with 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;

- informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil)
- 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 emergency)

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 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.

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 shames
- retina pattern
- iris pattern
- hand measurement

As biometric data is personally identifiable information, its processing has to comply with the UK Data Protection Act 2018/UK GDPR. Under the UK Data Protection Act 2018/UK GDPR 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.

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, they will adhere to the CCTV policy, published on the trusts website for the use of these cameras.

The trust does not need to ask individuals' permission to use CCTV but will make it clear where individuals are being recorded. 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 pupils 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 pupil. Where we don't need parental consent, we will clearly explain to the pupil 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 pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils 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 (eg. cameras and portable devices) are used to take photographs, no personal devices of employees should be used to take photographs of pupils.

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 digital, IT and data services and the designated safeguarding lead.

Photographs and videos should be transferred to trust IT systems (eg. 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.

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)

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. 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 all emails you hold about me" 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.

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 of 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 preferably by completing the trust's online subject access request form 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, the requester must be informed of this within one month of the request being received.

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;

- 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 to the ICO.

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, pupils 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 and ransomware.

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 the digital, IT and data services team immediately, who will liaise with the data protection officer.

Immediate action and response

On discovering that there has been a data breach/infringement you must notify the trusts digital, IT and data services 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, the digital, IT and data services 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 digital, IT and data services, 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 digital, IT and data services 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

Digital, IT and data services, 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.

- **Digital Innovator and technical lead:** 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.

- **Director of people:** The director of people will lead of any employee welfare or disciplinary issues, within the usual policy parameters.

- **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 digital, IT, data and data services (who will lisaise 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.

Accountability

The UK Data Protection Act 2018/UK GDPR requires the trust to have appropriate measures and records in place to demonstrate compliance with the act.

The trust demonstrates accountability in a number of ways including:

- Having appropriate policies in place
- Following data protection by design and default
- Using data processing agreements in contracts
- Maintaining records of processing activities
- Implementing technical and organisational security
- Managing data breaches
- Completing data protection impact assessments
- Having an appropriately skilled and knowledgeable data protection officer and team

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.