Data Protection Policy

Date created:	**February 2024**
Author:	**LCT Governance Professional**
Approved by:	**Resources Committee**
Date:	**11/03/24**
Next review date:	**March 2025**

Contents

1. Introduction

The Learning Community Trust (the Trust) aims to ensure that all personal data collected about pupils, staff, parents/carers, trustees, governors, 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.

2. Legislation and guidance

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
- UK Data Protection Act 2018 (DPA 2018)

It is based on guidance/Codes of Practice 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 regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreements and Articles of Association.

3. Definitions

The following terms are used throughout this policy:

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • 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's: • 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
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.
Trust	The Learning Community Trust, comprising the central trust team and its schools/academies.

4. The data controller

The Trust processes personal data relating to pupils, staff, parents/carers, trustees, governors, visitors and others. On behalf of the Trust, the Chief Executive Officer is the data controller.

The Trust is registered with the ICO and annually pays its registration fees, as legally required.

5. Roles and responsibilities

This policy applies to all staff employed by our Trust and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governance and accountability

The LCT Board (board of trustees) has overall responsibility for ensuring the Trust and its schools comply with all relevant data protection obligations.

5.2 Data protection officer (DPO)

All Trusts are required to have a data protection officer (DPO) under the UK General Data Protection Regulation (UKGDPR). The DPO should be:

- Independent
- Have an expert understanding of UK data protection law
- Report directly to the highest level of management
- Have adequate resources to carry out the role.

The Learning Community Trust outsources the role of DPO to ensure these criteria are met. The DPO provides advice and support to the Trust regarding data protection matters.

The DPO is the first point of contact for individuals whose data the Trust processes and for the ICO (as set out in Section 5.5).

The contact details for the DPO can be found in Appendix 1 of this policy.

5.3 The HR & Administration Compliance Officer

The Trust's HR & Administration Compliance Officer is responsible for overseeing the implementation of this policy, liaising with the DPO, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to trustees and, where relevant, report to their advice and recommendations on data protection issues. Compliance will include the annual completion of the Annual Accountability Framework Certificate provided by the DPO.

The HR & Administration Compliance Officer is the first point of contact regarding the operation of this policy and any concerns about compliance (as set out in Section 5.5).

The contact details for the HR & Administration Compliance Officer can be found in Appendix 1 of this policy.

5.4 Chief executive officer

The Trust's Chief Operating Officer (COO) acts as the representative of the data controller on a day-to-day basis.

5.5 All staff

Staff 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 DPO in the following circumstances:
    - With any questions about data protection law, retaining personal data or keeping personal data secure
    - 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, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach or incident
    - 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
- Contacting the HR & Administration Compliance Officer in the following circumstances:
    - With any questions about the operation of this policy
    - If they have any concerns that this policy is not being followed

6. Data protection principles

The UK GDPR is based on data protection principles that our Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

7. Collecting personal data

7.1 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 into 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, for example data relating to safeguarding, special and additional needs of our pupils and health data where appropriate for our pupils and staff members, 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 pupil) 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.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the 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 (where appropriate) inform the individuals concerned before we do so, and seek consent if necessary.

Staff must only process personal data where it is necessary in order to do their jobs or there is a legal basis for retention.

Staff members will only collect and process the minimum amount of personal data to achieve the objective in question.

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 and there is no legal basis for retention, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule.

A central register of all 'sub-processors' used by the Trust and its schools/academies will be kept and maintained by the HR & Administration Compliance Officer.

8. Sharing personal data

We may share personal data without consent if another legal basis applies. Situations where this may occur include, but are not limited to:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies (including the Department for Education) where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests (SAR)

Individuals have a right to make a 'subject access request' to potentially gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

SARs can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing (using the Trust's SAR template) and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff (or trustees/governors) receive a SAR in any form they must immediately forward it to the DPO, who will liaise with the HR & Administration Compliance Officer so they can coordinate the response.

A copy of the SAR template is made available alongside this policy on the LCT's website and internal SharePoint folders for trust-wide policies.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent (who has parental responsibility) or carer (with appropriate legal status) to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils at our primary schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils at our secondary schools may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Where a SAR relates to one of our specialist settings, the pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as 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 we can't reasonably anonymise, and we don't have the other person's 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

Additionally, there are a number of exemptions from the right of access that might apply in these circumstances.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

In the event of the release of a document being exempt, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see Section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational records

For our academies, there is no automatic parental right of access to the educational record of their child.

For our specialist settings, parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record only, the Trust may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18; however, the LCT extends this right to parents of children over the age of 18 where they are a pupil at one of our specialist settings.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Where our schools use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. A school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use a school's biometric system(s). We will ensure an alternative means of accessing the relevant services for those pupils is provided.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is 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's parent(s)/carer(s).

Where staff members or other adults use a school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

The school will complete a Data Protection Impact Assessment prior to implementing biometric processes.

12. CCTV

We use CCTV in various locations across the Trust to ensure its sites remain safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Where CCTV is in use at one of our sites, a CCTV Policy will be in place.

Any enquiries about the CCTV system should be directed to the LCT's Chief Operating Officer (see Appendix 1 for contact details).

13. Photographs, videos and telephone recordings

As part of our Trust activities, we may take photographs and record images of individuals within our schools.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.

Any photographs and videos taken by parents/carers at school/Trust 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 have agreed to this.

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

- Within schools or the Trust offices on notice boards and in magazines, brochures, newsletters etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns etc
- Online on our school/Trust websites or social media

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.

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.

See our schools' respective safeguarding policies for more information on our use of photographs and videos.

Phone calls are not recorded by the Trust and its schools.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Learning Community 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 personal data breach procedure (see Section 18).

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see Section 6)
- Completing data protection impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our Trust, its schools and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school/Trust office
- Passwords based on the latest guidance from the National Cyber Security Centre are used to access Trust computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils, trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for LCT-owned equipment (see our schools' online safety policies and the Trust's acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see Section 8)

17. Disposal of records

In compliance with the Trust's Data Retention Schedule, personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the Trust has an information/data breach procedure that should be followed., as set out in Appendix 2.

When the appropriate criteria is met, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a MAT/school context may include, but are not limited to:

- A non-anonymised dataset being published on a school's website, which shows the exam results of pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person
- The theft of a Trust laptop containing non-encrypted personal data about pupils

Staff who do not comply with this procedure may face disciplinary action.

19. Training

All staff, trustees and governors will be provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

20. Learning lessons

The HR & Administration Compliance Officer will refer any underlying issues raised by data incidents and breaches to the Headteachers/Principals, Executive team and/or the CEO of the LCT where appropriate, and respecting confidentiality, to determine whether there are any improvements that the Trust can make to its procedures or practice to help prevent similar events in the future.

21. Monitoring arrangements

The HR & Administration Compliance Officer is responsible for monitoring and reviewing this policy and will involve the Data Protection Officer to ensure the Trust remains compliant.

This policy will be reviewed annually and presented for approval to the Resources Committee of the LCT Board.

22. Links with other policies

This data protection policy is linked to our:

- Acceptable use of IT agreement
- Freedom of information publication scheme
- Data retention policy
- Individual schools' safeguarding and online safety policies
- Individual schools' biometric information and CCTV policies
- Information sharing policy
- Password management policy
- Records management policy

Appendix 1 – Contact details (as at March 2024)

HR & Administration Compliance Officer	dataprotection@lct.education 01952 387204
Data Protection Officer (DPO)	dpo@lct.education 01952 383103 / 07970 334500
Chief Operating Officer	LCTexecutive@lct.education 01952 387010

Appendix 2 – Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach or potential breach, the staff member, trustee, governor or data processor must immediately report the breach/potential breach by:

- Informing their line manager, verbally where possible, who in turn will advise the Headteacher/Principal (or the HR & Administration Compliance Officer if involving the Trust)
- Completing the Trust's data breach/potential breach notification form and sending it via email to the DPO (see Appendix 1 for contact details) within 24 hours. A copy of the notification form is made available alongside this policy on the LCT's internal SharePoint folders for trust-wide policies. The HR & Administration Compliance Officer should be copied into the email to ensure the Trust has been notified of the incident/breach
- Supported by the HR & Administration Compliance Officer where appropriate, the DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff, trustees and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will formally alert the LCT's HR & Administration Compliance Officer, who will advise CEO and LCT Board
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's IT network.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned

        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the Trust's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the Trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the Trust's IT network, including the templates completed in the event of an incident/breach.

- The DPO and HR & Administration Compliance Officer will meet as soon as reasonably possible to review what happened and how it can be stopped from happening again. The Data Protection Lead will then provide feedback to the Trust and the appropriate school(s)
- The HR & Administration Compliance Officer will record data incidents and breaches, identify any trends or patterns requiring action by the Trust to reduce risks of future breaches and report findings to the CEO and Resources Committee

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the Trust's IT provider to attempt to recall it from external recipients and remove it from the Trust's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the appropriate designated safeguarding lead and discuss whether any, or all, of the three local safeguarding partners should be informed

Other types of breach that you might occur in a trust/school setting include:

- Details of pupil premium interventions for named children being published on a school's website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A Trust laptop containing non-encrypted sensitive personal data being stolen or hacked
- A school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families