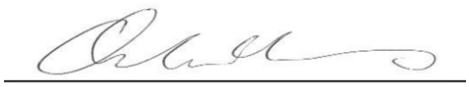
Central Region Schools Trust

Founded by the RSA

DATA PROTECTION POLICY

Recommended by:	Chief Operations Officer
Ratified by:	Trust Board
Signed:	
Position on the Board:	Chair
Ratification Date	**21.05.2025**
Next Review:	Summer Term 2026
Policy Tier (Central/Hub/School):	Central

Key Changes in the Latest Version of the Policy

- Section 2, without changing context.
- Section 5.2 – Removed reference to Teresa (Current DPO)
- Whole document – General formatting improvements.
- Section 5.7 – reworded without changing context.
- Section 5.8 – reworded without changing context.
- Section 5.9 – reworded without changing context
- Section 8 – reworded and reformatted
- Section 9.1 – Reworded paragraph regarding submitting SAR's as legally we have to allow a verbal request and this was not included. Reworded SAR request details to reference ID.
- 9.2 – reworded and added in a line reference potential fee for unfounded or excessive requests.
- 10 – I have removed this entire section as this is only for Maintained schools.
- Section 12 – removed reference to example articles and kept it factual (e.g. removed reference to DesignEd). Removed reference to CCTV footage as this is something users can't "opt out of" and CCTV is covered in section 11.
- Section 14 – Aligned wording with Online Safety Policy in regard to securing device when not in use, personal devices and strong passwords.
- Section 16 – updated wording to improve clarity and readability. E.g. highlight threshold for reporting to ICO and clearly define the process followed.
- Section 18 –removed Internal Auditor from here and just stated the policy will be reviewed annually and shared with trust board for ratification.
- Section 19 – policy wording was incorrect for Online Safety Policy. Also referred to a policy which does no longer exist which has been removed.
- Section 20 – removed reference to Internal Auditor and setup a generic email address which I will monitor / share with Internal Auditor

1. AIMS

The Central Region Schools Trust (the Trust) aims to ensure that all personal data pertaining to staff, pupils/students, parents, Trustees, Governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

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

2. LEGISLATION AND GUIDANCE

This policy is designed to meet the requirements of the UK GDPR and the DPA 2018, as well as the guidance provided by the Information Commissioner's Office (ICO) on GDPR compliance and the ICO's Code of Practice for Subject Access Requests.

In addition to complying with the relevant data protection legislation, the Trust also adheres to the Protection of Freedoms Act 2012 concerning the use of biometric data and maintains compliance with the ICO's guidelines regarding the use of surveillance cameras and personal information. Furthermore, this policy aligns with our Funding Agreement and Articles of Association, ensuring compliance across all frameworks.

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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 of 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.

4. THE DATA CONTROLLER

The Trust processes personal data relating to parents/carers, pupils/students, staff, Trustees, Governors, visitors and others, and therefore is a Data Controller.

The Trust is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

The Trust has delegated responsibility to the Principal in each school for ensuring compliance with the UK GDPR and this policy within the day-to-day activities of the school. Where there is an Executive Principal, this is delegated to the Head of School.

5. ROLES AND RESPONSIBILITIES

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

5.1 Trust Board

The Central Region Schools Trust Board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

Our DPO oversees policy implementation, monitors compliance with data protection laws, and offers guidance. They report annually to the Trust Board and act as the primary point of contact for data subjects and the ICO.

5.3 Executive Principal (CEO)

The Executive Principal (CEO) is responsible for ensuring that the data protection policy and guidelines are being adhered to.

5.4 Principal/Head of School

The Principal/Head of School in each school acts as the representative of the Data Controller on a day-today basis.

5.5 Trust Data Manager

The Trust Data Manager supports the DPO, oversees the implementation of this policy and other related policies across the Trust, monitors the schools' compliance with data protection law and provides training to the GDPR Leads in line with the DPO's guidance.

The Trust Data Manager acts as the GDPR Lead for the Executive Leadership and Central Teams.

5.6 GDPR Lead

Each school in the Trust has a designated GDPR Lead responsible for:

- Supporting the DPO and Trust Data Manager.
- Overseeing the implementation of this policy and the Records Management Policy.
- Monitoring the school's compliance with data protection law.
- Reporting any breaches to the DPO.
- Being vigilant to potential risks to personal data, such as:
    - New projects/data processing activities.
    - Unsecured computer screens. ○ Confidential papers left on vacant desks.
    - Unauthorized use of photographs/sharing of data.

- Retention of data for longer than necessary.
- Ensuring that all members of staff receive GDPR training.
- Ensuring that any Data Protection Impact Assessments (DPIAs) are completed and filed.

5.7 Information Asset Owners

Each school, as well as the Executive and Central Teams, will appoint Information Asset Owners (IAOs) responsible for managing various types of data. These IAOs are tasked with identifying and mitigating risks to the information they oversee. They must have a comprehensive understanding of the data, including its purpose, history of modifications, and authorized access. Additionally, IAOs ensure the protection of information through appropriate security measures such as password protection and encryption. For further details, please consult the Records Management Policy.

5.8 All staff

Staff are responsible for:

- Collecting, storing, and processing personal data in accordance with this policy.
- Promptly informing the Trust of any changes to their personal data, such as address or phone number updates.
- Contacting the Data Protection Officer (DPO) or relevant GDPR Lead in the following instances: ○ Seeking clarification on policy operations, data protection laws, or maintaining data security.
  - Reporting concerns regarding policy adherence.
  - Seeking guidance on lawful basis for personal data usage, consent management, privacy notices, data rights, or cross-border data transfers.
  - Reporting data breaches or engaging in activities affecting individuals' privacy rights.
  - Seeking assistance with contracts or sharing personal data with third parties.

5.9 Parents/Carers

Parents/carers are expected to:

- Verify the accuracy and currency of information provided to the relevant school within the Trust. ○ Promptly notify the relevant school of any changes to their provided information, such as address or telephone number modifications.
- Inform the relevant school of any inaccuracies in the information maintained by the school. It's essential to note that while the Trust strives to maintain accurate records, it relies on timely updates from parents/carers, and it cannot be held responsible for errors unless informed.

6. DATA PROTECTION PRINCIPLES

The UK GDPR is based on data protection principles that the 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 one 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-eg 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,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust 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/student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

If we offer online services to pupils/students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil/student is under 13 (except for online counselling and preventive services).

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

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 inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

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 Records Management Policy.

8. SHARING PERSONAL DATA

This section outlines the circumstances under which personal data may be shared by the Trust, ensuring compliance with data protection laws and safeguarding individuals' rights:

- Routine Sharing: Personal data will not typically be shared unless under specific circumstances:
- Instances where the safety of staff is at risk due to issues involving pupils/students or parents/carers.
- Liaison with external agencies, with consent sought as necessary.
- Sharing with suppliers or contractors for service provision, contingent upon:
- Suppliers or contractors guaranteeing compliance with data protection laws.
- Establishment of a Data Sharing Agreement to ensure fair and lawful processing.
- Sharing only necessary data for service provision and safety.

- Legal Obligations: Personal data may be shared with law enforcement and government bodies when legally required for:
- Crime and fraud prevention or detection.
- Apprehension or prosecution of offenders.

- Tax assessment or collection owed to HMRC.
- Legal proceedings or safeguarding obligations.
- Research and statistical purposes, ensuring sufficient anonymization or obtaining consent.

- Emergency Situations: Personal data may be shared with emergency services and local authorities to respond to emergencies involving pupils/students or staff.

- International Transfers: Personal data transfers outside the UK will comply with data protection laws.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject Access Requests

Individuals have a right to make a 'Subject Access Request' to 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
- 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

Subject Access Requests (SARs) can be submitted verbally or in writing, in accordance with GDPR law. For written submissions, individuals are encouraged to use the "Subject Access Request Form" available on our websites. Completed forms can be sent to the following address: Central Region Schools Trust, B.06 Assay Studios, 141-143 Newhall Street, Birmingham, B3 1SF, or via email to dpo@crst.org.uk

Subject Access Requests should include:

- Full name of the individual making the request.
- Contact details for correspondence.
- Sufficient information to confirm the identity of the requester, such as providing identification documents if requested.
- Details of the specific information or data being requested, including relevant dates or time periods if applicable.
- Any additional information or context that may help locate the requested data.

If staff receive a Subject Access Request they must immediately forward it to the Trust Data Manager and DPO.

9.2 Responding to Subject Access Requests When responding to requests, we:

- May request two forms of identification from the individual.
- May contact the individual via phone to verify the request.
- Will promptly respond within one month of receiving the request.
- Will provide the requested information free of charge, except in cases where the request is manifestly unfounded or excessive, or if the individual requests further copies of their data following a previous request.
- May notify the individual of a three-month response period for complex or numerous requests, providing an explanation within one month of receipt.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil/student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

For unfounded or excessive requests, we may refuse or charge a reasonable fee, considering administrative costs. Such requests include repetitive or duplicative inquiries. We inform individuals of refusal reasons and their right to complain to the ICO.

9.3 Other data protection rights of the individual

In addition to the right to submit a Subject Access Request and receive information during data collection (as outlined in section 7), individuals possess the following rights:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the UK
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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 wishing to exercise these rights should direct their requests to the Data Protection Officer (DPO). In the event that staff members receive such requests, they are required to promptly forward them to the Trust Data Manager and DPO for processing.

10. BIOMETRIC RECOGNITION SYSTEMS

Where we use pupils'/students' biometric data as part of an automated biometric recognition system (for example, pupils/students use fingerprints 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. The Trust 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/students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils/students. For example, pupils/students can be given a 4-digit PIN to pay for school dinners if they wish.

Parents/carers and pupils/students can object to participation in the school's biometric recognition system(s), or 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/student 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/student's parent(s)/carer(s).

Where staff members or other adults use the 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 Trust will delete any relevant data already captured.

11. CCTV

We use CCTV in various locations around some of the Trust's school sites to ensure it remains safe. We will adhere to the ICO's Code of Practice for the use of CCTV.

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.

All CCTV footage will be kept in accordance with the Trust's Records Management Policy for security purposes. The Network Manager/Site Manager is responsible for keeping the records secure and allowing access.

Any enquiries about the CCTV system should be directed to the Principal/Head of School.

12. PHOTOGRAPHS AND VIDEOS

We may take photographs and record images of individuals, as part of our day-to-day activities within the Trust and its schools.

We will obtain written consent from parents/carers, or pupils/students aged 18 and over, for photographs and videos to be taken of pupils/students 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 pupil/student. Where we don't need parental consent, we will clearly explain to the pupil/student how the photograph and/or video will be used.

Uses may include:

- For the profile picture on the school or Trusts IT systems
- For GCSE and A Level examination submissions
- Performing arts including dance and movement, concerts and drama performances
- Sports days and sports fixtures and the use of photographic equipment by parents/carers
- Media, including newspapers and television
- Displays in schools and the Trust's office
- The Trust and school publications
- The Trust and school websites
- The Trust and school social media accounts
- Staff training and professional development activities

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 of individual pupils/students, we will not accompany them with any personal information about the child, to ensure they cannot be identified.

See our Safeguarding and Child Protection Policy for more information on our use of photographs and videos.

13. 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 Privacy Impact Assessments (DPIAs) 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 • Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

14. DATA SECURITY AND STORAGE OF RECORDS

We are committed to safeguarding personal data to prevent unauthorized access, alteration, processing, or disclosure, as well as 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 securely stored when not in use.
- Confidential papers containing personal data must not be left unattended on office or classroom desks, staff room tables, notice boards, or any other accessible areas.
- All members of staff have a secure login protected with multi-factor authentication and credentials must not be shared with other users.
- All staff are required to use a strong password in accordance with recommendation from the National Cyber Security Centre (NCSC).
- All staff devices are encrypted to protect data in the event of loss or theft.
- Documents containing sensitive or confidential information are password-protected or if there are unsecure servers between the sender and the recipient.
- Staff and volunteers who use personal devices are expected to follow the same security procedures as for school-owned equipment as detailed in our Online Safety Policy and 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)
- Where personal information is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security. The person taking the information for the school premises accepts full responsibility for the security of the data.

15. DISPOSAL OF RECORDS

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.

16. PERSONAL DATA BREACHES

Central Region Schools Trust is committed to maintaining the highest standards of data protection and privacy for all individuals associated within our trust and we will adhere to the procedure outlined in appendix 1 below. In the event of a suspected or confirmed personal data breach, swift and effective action will be taken to mitigate risks and ensure compliance with applicable data protection laws. If the breach is determined to meet a severity threshold and has the potential to impact individuals' rights and freedoms, we will promptly report this to the Information Commissioner's Office (ICO) within 72 hours. Our reporting process aims to ensure compliance with legal requirements and mitigate any adverse effects on data subjects.

Our breach management procedures below are designed to promptly identify, assess, and address any breaches of personal data within our trust.

1. Reporting Procedure:
    - Any individual who suspects or becomes aware of a personal data breach must immediately report it to the designated Data Protection Officer (DPO) or school GDPR Lead.
    - Upon receiving a report of a breach, the DPO or GDPR Lead will initiate an internal investigation to assess the nature and scope of the breach.
2. Assessment and Mitigation:
    - The internal investigation will include an assessment of the severity and potential impact of the breach on individuals' rights and freedoms.
    - Immediate steps will be taken to contain the breach and prevent further unauthorized access or disclosure of personal data.
    - Our team will assess the risks associated with the breach and implement appropriate measures to mitigate these risks, including notifying affected individuals where necessary.
3. Notification to Supervisory Authority and Data Subjects:
    - If a breach is determined to pose a risk to individuals' rights and freedoms, we will promptly notify the relevant supervisory authority, such as the Information Commissioner's Office (ICO), in accordance with legal requirements.
    - Affected individuals will be notified directly of the breach if it is likely to result in a high risk to their rights and freedoms. This notification will include relevant information about the breach, its potential consequences, and steps they can take to mitigate any adverse effects.
4. Review and Remediation:
    - Following the resolution of a breach, we will conduct a thorough review of the incident to identify any underlying causes or weaknesses in our data protection practices.
    - Remedial actions will be implemented to address any identified vulnerabilities and strengthen our data protection measures, including additional staff training or policy updates.

17. TRAINING

All staff, Trustees and governors are 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.

18. MONITORING ARRANGEMENTS

This policy will be reviewed and updated, if necessary, every year and shared with the full Trust Board for ratification.

19. LINKS WITH OTHER POLICIES

This Data Protection Policy is linked to our:

- Freedom of Information Policy
- Staff Code of Conduct
- Online Safety Policy
- Safeguarding and Child Protection Policy
- Records Management Policy

20. CONTACT US

- **Address:** The Central Region Schools Trust, B.06 Assay Studios, 141-143 Newhall Street, Birmingham, B3 1SF
- **Telephone number:** 0121 270 3117
- **Email:** dpo@crst.org.uk

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

Procedure for personal data breaches in a school

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the relevant GDPR Lead who will alert the DPO and take advice regarding the investigation.
- The relevant GDPR Lead will investigate the report and determine whether a breach has occurred. To decide, they 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

The relevant GDPR Lead will alert the Principal/Head of School. The Principal/Head of School will alert the chair of governors.

- The relevant GDPR Lead will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DPO and relevant GDPR Lead will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a caseby-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (eg emotional distress), including through:
  - ○ Loss of control over their data ○ Discrimination ○ Identify theft or fraud ○ Financial loss
  - ○ Unauthorised reversal of pseudonymisation (for example, key-coding) ○ Damage to reputation Loss of confidentiality
  - ○ Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the GDPR in Schools (GDPRiS) Management System.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. 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. 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

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - ○ 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 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 GDPR in Schools (GDPRiS) Management System

- The DPO, Principal/Head of School and relevant GDPR Lead will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Procedure for personal data breaches from the Executive or Central Team

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the relevant GDPR Lead who will alert the DPO and take advice regarding the investigation.
- The relevant GDPR Lead will investigate the report and determine whether a breach has occurred. To decide, they 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

The relevant GDPR Lead will alert the Chief Operating Officer. The Chief Operating Officer will alert the Executive Principal (CEO) and Chair of the Trust Board.

- The relevant GDPR Lead will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DPO and relevant GDPR Lead will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a caseby-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (eg emotional distress), including through:
  - Loss of control over their data ○ Discrimination ○ Identify theft or fraud ○ Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding) ○ Damage to reputation Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the GDPR in Schools (GDPRiS) Management System.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. 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. 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

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - 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 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 GDPR in Schools (GDPRiS) Management System

- The DPO, Chief Operating Officer and relevant GDPR Lead will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.