Creative Education Trust

Data Protection Policy

Policy Owner	Data Protection Officer
Approved by	Audit and Risk Committee
Last reviewed on	November 2024
Next review date	November 2026

Data Protection Policy

Contents

1. Introduction

1.1 Creative Education Trust aims to ensure that all personal data about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed by the Trust in accordance with the General Data Protection Regulation (GDPR)[1] and the Data Protection Act 2018 (DPA 2018).

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

2. Legislation and guidance

2.1 This policy meets the requirements of the GDPR and the DPA 2018. It is based on current guidance published by the Information Commissioner's Office (ICO) on the GDPR[2] and the ICO's code of practice for subject access requests[3].

2.2 This policy also meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data in schools.

2.3 This policy also reflects the ICO's code of practice for the use of surveillance cameras i.e. CCTV and personal information.

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

3. Definitions

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

[1] http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf
[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
[3] https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

	• 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 that is done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing may 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

4.1 Creative Education Trust processes personal data relating to parents, pupils, staff, governors, visitors, and others, and therefore is a data controller.

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

5. Scope

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

6. Roles and responsibilities

6.1 The Board of Directors

6.1.1 The Board of Directors of Creative Education Trust has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

6.2 The Data Protection Officer (DPO)

6.2.1 The DPO is responsible for overseeing the implementation of this policy, monitoring Creative Education Trust's compliance with data protection law, and developing related policies and guidelines where applicable.

6.2.2 The DPO will provide an annual report of activities directly to the Board of Directors and, where relevant, report to the board advice and recommendations on school data protection issues.

6.2.3 The DPO is the point of contact with the ICO and will offer advice and guidance to school data protection leads.

6.2.4 The Trust is compliant in having a DPO registered with the Information Commissioner and is and is contactable via dpo@creativeeducationtrust.org.uk or by post at the following address: Data Protection Officer, Creative Education Trust, 67-68 LONG ACRE, LONDON WC2E 9JD.

6.3 Principal/Headteacher

6.3.1 The Principal/Headteacher acts as a representative of the data controller on a day-to-day basis.

6.4 School Data Protection Leads

6.4.1 School data protection leads are the first point of contact and advice for any data protection concerns or issues at school level.

6.4.2 Details of the individual school's data protection lead will also be available from each school office.

6.5 All employees

6.5.1 Employees are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy.
- Ensuring that any personal data they provide to the school (for example, their contact details) is accurate.
- Informing the school of any changes to their own personal data, such as a change of address.
- Being mindful of the fact that individuals have the right to see their 'personal data'. Therefore, employees should not record comments or other data

about individuals, which they would not be comfortable in the individual seeing, either in emails or elsewhere.
- Not covertly or without permission recording (video or audio) pupils, staff, or other individuals.
- Only ever obtaining or using personal data relating to third parties for approved work purposes.
- Taking appropriate initial action to minimise the impact of a potential data breach. e.g., if an email containing personal data has been sent to an incorrect recipient, the email must be recalled immediately, and the school data protection lead and IT informed.
- Contacting the school data protection lead in the first instance in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
    - 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.
    - If they find any lost or discarded data which they believe contains personal data, (for example, may include a memory stick).
    - If they become aware that personal data has been accidentally lost or stolen or inadvertently disclosed. For example, if their laptop is stolen or their phone is lost, and it has personal data stored on it.

6. Data protection principles

6.1 The GDPR is based on data protection principles that all organisations must comply with.

6.2 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.

6.3 This policy sets out how Creative Education Trust and each of its schools aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness, and transparency

7.1.1 Personal data will only be processed, where one of 6 'lawful bases' (legal reasons) exists to do so under data protection law:

- The data needs to be processed so that Creative Education Trust or an individual school can **fulfil a contract** with the individual, or the individual has asked the Trust or school to take specific steps before entering a contract.
- The data needs to be processed so that the Trust or school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g., to protect someone's life.
- The data needs to be processed so that the Trust or school, 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 school 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.**

7.1.2 For special categories of personal data, we will also meet one of the special category conditions under data protection law.

- The individual (or their parent/carer when appropriate in the case of a pupil) has given 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 need 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 of substantial public interest as defined in legislation.
- The data needs to be processed for health or social care purposed 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 archiving purposes, scientific or historical research purposes or statistical purposes and the processing is in the public interest.

7.1.3 For criminal offense 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.

7.1.4 At the Trust's primary schools, if online services are offered to pupils, such as classroom apps, and the school intends to rely on consent as a basis for processing, parental consent will be obtained (except for online counselling and preventive services).

7.1.5 At the Trust's secondary schools, if online services are offered to pupils, such as classroom apps, and the school intends to rely on consent as a basis for processing, parental consent will be obtained where the pupil is under 13 (except for online counselling and preventive services).

7.2 Limitation, minimisation, and accuracy

7.2.1 Personal data will only be collected for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when their data is first collected.

7.2.2 If Creative Education Trust or one of its schools wishes to use personal data for reasons other than those given when it was first obtained, the individuals concerned will be informed before this takes place, and consent sought where necessary.

7.2.3 Staff must only process personal data where it is necessary to do their jobs. When staff no longer need the personal data they hold, they must ensure it is appropriately deleted. This will be done in accordance with Creative Education Trust's Records Management Policy.

7.2.4 The Trust's schools will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate in relation to the Trusts Records Management Policy.

8. Sharing personal data

8.1 Personal data will not normally be shared with any other parties. However, exceptions to this are where:

- There is an issue with a pupil or parent/carer that puts the safety of Creative Education Trust's staff at risk.

- The Trust or the school need to liaise with other agencies. If required, consent will be sought in advance.
- The Trust or school or individual suppliers or contractors need data to enable the provision of services to our staff and pupils – for example, IT companies. When doing this, the Trust and individual schools will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data that is shared.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust or the school.

8.2 Creative Education Trust and individual schools will also share personal data with law enforcement and government bodies where there is a legal requirement to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, if personal data is sufficiently anonymised, or consent has been provided

8.3 Creative Education Trust and individual schools may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of the Trust's pupils or staff.

8.4 Where personal data is transferred to a country or territory outside the European Economic Area, this will be done in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

9.1.1 Individuals have a right to make a 'subject access request' to gain access to personal information that is held 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

9.1.2 Subject access requests Individuals can make a subject access request in any forma, but it must be made to the school data protection lead and copied to the Creative Education Trust's DPO. Requests should include:

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

9.1.3 If staff receive a subject access request, they must immediately forward it to the school data protection lead and the DPO.

9.2 Children and subject access requests

9.2.1 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.

9.2.2 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 or carers of pupils attending Creative Education Trust 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.

9.2.3 Children aged 12 and above 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 carers of pupils attending Creative Education Trust 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.

9.3 Responding to subject access requests

9.3.1 When responding to requests:

- The individual may be asked to provide two forms of identification.
- The individual may be contacted via telephone to confirm the request was made.
- The Trust or individual school will respond without delay and within one month of receipt of the request.
- The information will be provided free of charge.
- If the request is complex or numerous, the individual may be told that we will comply within three months of receipt of the request. The individual will be informed of this within one month and provided with an explanation of why the extension is necessary.

9.3.2 Information may 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 is at risk of abuse, but only in situations where the disclosure of such information would not be in the child's best interests
- Includes another person's personal data, unless such personal data can be reasonably anonymised or the person whose personal data is included provides consent to their data being disclosed.
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Forms part of sensitive documentation, including but not limited to those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

9.3.3 If the request is unfounded or excessive, the Trust or individual school may refuse to act on it or charge a reasonable fee which considers administrative costs. See guidance from the ICO on where charges may be applicable. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-should-we-consider-when-responding-to-a-request/#fee

9.3.4 A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

9.3.5 When a request is refused, the individual will be provided with the reasons for the refusal and informed of their right to complain to the ICO.

9.4 Other data protection rights of the individual

9.4.1 In addition to the right to make a subject access request (see above), and to receive information when data is being collected, about how it is used and processed (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask the Trust or the individual school 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 based on public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- 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).

9.4.2 Individuals should submit any request to exercise these rights to the data protection lead at the school copying the DPO. If staff receive such a request, they must immediately forward it to the school's data protection lead and copy it to the DPO.

10. Parental requests to see the educational record

10.1 There is no automatic parental right of access to the educational record in academies, including free schools. If a parent wishes access to the educational record, then they should follow the subject access request process as set out in section 9.

11. Biometric recognition systems

11.1 Where pupils' biometric data is used as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012. In the context of the Protection of Freedoms Act 2012, a 'child' means any individual under the age of 18.

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

11.3 Parents/carers and pupils have the right to choose not to use the school's biometric system(s). The school will provide alternative means of accessing the relevant services for those pupils.

11.4 Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the school will make sure that any relevant data already captured is deleted.

11.5 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, that data will not be processed irrespective of any consent given by the pupil's parent(s)/carer(s).

11.6 Where staff members or other adults use the school's biometric system(s), their consent will also be obtained before they first use the system. Adults will also be provided with 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.

12. CCTV

12.1 Creative Education Trust schools use CCTV in various locations around school sites to ensure they remain safe and secure. When CCTV is used, the school will adhere to the ICO's code of practice for the use of CCTV.

12.2 It is not necessary to ask individuals' permission to use CCTV, but each school will make it clear where individuals are being recorded. Security cameras will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

12.3 Any enquiries about the CCTV systems within Trust schools should be directed to the individual school's data protection lead in the first instance.

13. Photographs and videos

13.1 As part of school and Creative Education Trust activities, photographs may be taken, and images recorded of individuals.

13.2 In the Trust's primary schools, written consent will be obtained 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 pupil.

13.3 In the Trust's secondary schools, written consent will be obtained 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 parental consent is required, it will be clearly explained how the photograph and/or video will be used to both the parent/carer and pupil. Where it is not necessary to gain parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

13.4 Uses may include:

- Within the individual pupil's school or other Creative Education Trust schools or the Trust's offices on notice boards and in school and Trust magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on the school or Trust website or social media pages

13.5 Consent can be refused or withdrawn at any time. Where consent is withdrawn it may not always be possible for the school or the Trust to remove all images of the pupil from communication, marketing, and promotional materials.

13.6 If the school or Creative Education Trust wish to use a pupil's image linked to their full name (for example, a pupil child being named in press/literature to celebrate an achievement), parents will be contacted separately for permission.

14. Data protection by design and default

14.1 Measures will be put in place to show that data protection has been integrated into all the Creative Education Trust's 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 privacy impact assessments where the Trust's or the individual school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Training staff on data protection.
- Regularly conducting reviews and audits to test privacy measures and ensure compliance.
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school data protection lead and the Trust's DPO and all information that Creative Education Trust is required to share about how their personal data is used and processed (via individual 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.

15. Data security and storage of records

15.1 Personal data will be protected and kept safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage. Members of staff must read and adhere to the E-Safety Policy and Online Safety Policy in relation to the security of electronic records.

Employees should take appropriate steps to ensure the security of paper records for example, through locking away confidential papers when not in use, and ensuring confidential data is not left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access. Staff, pupils, Trustees, governors, and volunteers who store personal information on their personal devices must follow the same security procedures as for school-owned equipment.

All staff, pupils' governors and volunteers must abide by this Data Protection Policy as well as Creative Education Trust's other policies including E-Safety Policy and the Online Safety Policy Where we need to share personal data with a third party, we will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

Where personal information needs to be taken off site, staff must sign it in and out from the school office.

16. Disposal of records

16.1 Personal data that is no longer needed will be disposed of securely. For further details, see Creative Education Trust's Records Management Policy.

17. Personal data breaches

17.1 The Trust and each individual school will make all reasonable endeavours to ensure that there are no personal data breaches.

17.2 In the unlikely event of a suspected data breach, the procedure set out in appendix 1 will be followed.

17.3 When appropriate, data breaches will be reported to the ICO within 72 hours.

17.4 Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school 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 school laptop containing non-encrypted personal data about pupils.

18. Training

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

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

19. Monitoring arrangements

19.1 The DPO is responsible for monitoring and reviewing this policy.

19.2 This policy will be reviewed and updated if necessary.

20. Links with other policies

20.1 This data protection policy is linked to our:

- Freedom of Information Policy and Publication Scheme
- Online Safety Policy
- Records Management Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches[4] produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the school data protection lead.
- The school data protection lead will immediately inform the Principal or Headteacher, the Trust's DPO and all other necessary individuals.
- 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
- The DPO will alert the Headteacher/Principal, Director of Finance, and all necessary individuals.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by other relevant staff members or data processors where necessary (actions relevant to specific data types are set out 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.
- The DPO will work out whether the breach must be reported to the ICO. This will be judged on a case-by-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 (e.g., 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 is likely that there will be a risk to people's rights and freedoms, the DPO will notify the ICO.
- The DPO will ensure that the decision is documented by the data protection lead / DPO in the Trusts GDPR Compliance tool in case it is challenged later by the ICO, or an individual affected by the breach.

[4] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

- 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 and 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 by the DPO on the Trusts GDPR Compliancy tool.

- The DPO and all other necessary individuals will review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving risky or sensitive information. We will review the effectiveness of these actions and amend them, if necessary, after any data breach.

Example below:

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 [ICT department to attempt to recall it from external recipients and remove it from the school'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 endeavour 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