Astrea Academy Trust

Data Protection Policy 2023-25

Date	6 September 2023
Written by	Data Protection Officer
Adopted by Trustees	20 June 2023
Review Date	June 2025, for September 2025

Contents

1. Aims

Astrea Academy Trust and its academies aim to ensure that all personal data collected about staff, pupils, parents, trustees, local committee members, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (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 meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data where used on Astrea Academy Trust premises.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information where used on Astrea Academy Trust premises.

Astrea Academy Trust also has regard to the DfE's advice on disputes relating to parental responsibility and information sharing/consent (see p7-9).

In addition, this policy complies with our Funding Agreement 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 • 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 (Including special educational needs, allergies and/or medical conditions) • 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 Academy Trust processes personal data relating to parents, pupils, staff, volunteers (including non-executives), visitors and others, and therefore is a data controller.

The Academy Trust is registered with the ICO and will renew this registration annually, along with relevant Data Protection fee as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Academy 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 Astrea Academy Trust Board

The Trust Board has overall responsibility for ensuring that our academies comply with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, 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 the Trust Board, via the Trustee Finance, Risk and Audit Committee, and, where relevant, report to the Board their advice and recommendations on academy data protection issues.

The DPO is also the first point of contact for individuals whose data the academy/trust processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Melanie Basson, Information and Governance Officer, and is contactable via our Sheffield office.

The Quadrant

99 Parkway Avenue

Sheffield

S9 4WG

Email: DPO@astreaacademytrust.org

The Data Protection Lead (DPL) responsible for the day to day data protection matters at Carrfield Primary Academy is:

Emma Fisher

emma.fisher@astreacarrfield.org

5.3 Principal

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

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the academy of any changes to their personal data, such as a change of address and contact details
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to collect and or store/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
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals, including the use of a new data processor and the upload of data to third party companies such as new learning platforms requiring students to log in
    - If they need help with any contracts or sharing personal data with third parties
    - If they need to apply a UK GDPR principle to processing data.

6. Data protection principles

The GDPR is based on data protection principles that our Trust and its academies 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 and its academies aim to comply with and remain accountable for demonstrating compliance 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 academy can **fulfil a contract** with the individual, or the individual has asked the academy to take specific steps before entering into a contract
- The data needs to be processed so that the academy 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 academy, 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 academy (where the processing is not for any tasks the academy performs as a public authority) or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/ carer when appropriate in the case of a pupil) has freely given clear **consent**

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

- 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.

If we offer online services to pupils, such as classroom apps, and we intent to rely on consent as a basis for processing, we will obtain parental consent where the pupil is under 13 (except for online counselling and preventative services.

7.2 Limitation, minimisation, retention 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 job.

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the academy's record retention schedule as defined by the Information and Records Management Toolkit for Schools.8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of **our staff** or pupils 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 which can provide sufficient guarantees that they comply with 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 where we are legally required 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
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of academy trips
- To provide information to another educational establishment to which a pupil is transferring
- Research, historical and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
- To provide information to the Examination Authority as part of the examination process

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The academy provides the relevant government departments with anonymised pupil data which is used for statistical or research purposes.

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, staff, volunteers, local committee members or visitors.

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

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 academy 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

Subject access requests can be submitted in any form, but we will be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form they must immediately forward it to the academy Data Protection Lead who must inform the DPO.

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 or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 13 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 at our academy 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 by the academy Principal.

The Principal must not refuse a request from a child with Special Educational Needs or Disability (SEND) solely on the basis of his or her SEND characteristic – any such request must be treated according to the individual circumstances of the child.

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 will not disclose information 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 cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it
- Would contravene exemptions as established in the Act, for example if disclosure would adversely affect the rights and freedoms of others or jeopardise police investigations into any alleged offence(s)

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.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they may subsequently 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:

- **Be informed** where their personal data is processed (Privacy Notices)
- **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** which 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 things about an individual based on their personal data with no human involvement)
- 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 –**Portability** (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 record

Parents, or those with parental responsibility, have a right under this policy to access to their child's educational record (which includes most information about a pupil) within 30 school days of receipt of a written request.
If the request is for a copy of the educational record, the academy may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might 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 we 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. The academy 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 the academy's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash or using an online payment system where available.

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 the academy'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 academy will delete any relevant data already captured.

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

12. CCTV

We use CCTV in various locations around the academy site to ensure it remains safe. We will adhere to the ICO's guidance for the use of CCTV.

CCTV imagery will be retained only as long as is necessary, for a minimum period of 5 calendar days and a maximum period of 6 months unless it is footage which relates to an incident under review.

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.

Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

Any enquiries about the CCTV system should be directed to the Data Protection Officer.

Any requests for disclosure of CCTV imagery MUST be directed to the Data Protection Officer.

13. Photographs and videos

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

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

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. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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.

Any photographs and videos taken by parents/carers at academy 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.

Some lessons may be recorded for teacher training purposes; the academy is not required to obtain permission for this.

Where we take photos of visitors within our academies using a secure digital sign-in system, we will not ask for any sensitive data, other than individuals name and car registration which we ask as part of Health and Safety.

14. 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 privacy impact assessments where the academy'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 academy 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

15. 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, communication or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops, hard drives and storage devices that contain personal data kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on display in offices and classrooms in staffrooms, pinned to notice/display boards, or left anywhere else where there is general public access. All staff are expected to operate a clear desk policy.
- **Where personal information needs to be taken off site, staff are responsible for the application of this policy whilst transporting off site and in their home environment.**
- **Paper based records containing significant amounts of sensitive information about one or more children must be signed out of the academy at the main office and signed back in upon return. Records must include staff member's name, date removed, type of data, date replaced.**
- Passwords that are at least 12 characters long containing a combination of upper and lower-case letters, numbers and symbols are used to access academy computers, laptops and other electronic devices. Passwords used are not a word that can be found in a dictionary or the name of a person, character, product, or organisation.
- Staff and pupils are advised to change their passwords at regular intervals which are significantly different from previous passwords.
- Staff and pupils are advised to use different passwords for each platform/application
- Staff and pupils are advised not to share their passwords with anyone else
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Use of the Trust's online platform is essential
- When data is shared using Office 365, through Sharepoint and OneDrive, this should be done carefully and reviewed regularly
- Staff, pupils and non-executives will store academy data on areas of devices backed up to academy servers or Astrea online platforms. Under no circumstances should devices (not backed up to academy servers) or USB sticks be used as the sole place to store academy data.
- The use of data storage/removable storage across the Trust is limited to the IT Manager and Technicians only or with the explicit permission of the Principal.
- All staff and pupils who wish to store personal academy information on their personal devices **Must**-have this authorised by their acting data controller (Principal) and use only Astrea Trust approved systems. Personal devices will be suitably encrypted and secured and not shared for use with non Astrea Trust employees. Data stored on personal devices will be shared with the academy and then permanently destroyed upon leaving Astrea Trust employment or the individual will be held personally liable. Academies procuring or using third party systems will have them authorised at Trust level before transmitting Trust data.
- 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)
- Staff, governors and volunteers are not permitted to remove/copy/download/publish/print data from any Astrea Academy Trust device or system without explicit consent from Astrea Academy Trust. Further details regarding security of IT systems are detailed in our Acceptable ICT Use policy

- Staff are advised to take extra care to protect individuals' personal information when communicating with parents, carers and outside agencies to ensure the correct recipient email address is used.

16. Disposal of data

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 academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

The disposal of data will be undertaken in accordance with the academies record retention schedule as defined by the Information and Records Management Toolkit for Schools.

17. Personal data breaches

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

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in an academy context may include, but are not limited to:

- A non-anonymised dataset being published on the academy 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 Trust or academy laptop containing non-encrypted personal data about pupils

18. Training

All staff and non-executives 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 academy's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy, which will be reviewed **every 2 years** and shared with the full Board of Trustees.

20. Links with other policies

This data protection policy is linked to our:

Freedom of information publication scheme

Safeguarding Policy

Acceptable ICT Use

Privacy Notices

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or academy Data Protection Lead must immediately notify the DPO submitting all relevant information using Athena online reporting system.
- 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 Principal. The Chair of the Finance, Risk and Audit Committee will be routinely informed of all data breaches reported to the ICO and the DPO may alert the Chair immediately of any reportable breach where necessary. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by 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 must 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's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO and the Chair of the Finance, Risk and Audit Committee.

- 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 using Athena online system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or through their breach report line (0303 123 1113) 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:
    - 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 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 using Athena online system.

As above, any decision on whether to contact individuals will be documented by the DPO.

The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, 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 ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will 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 ensure we receive 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 in a timely fashion as necessary according to the circumstances.