DATA PROTECTION POLICY

February 2023

Date approved:	27 March 2023
Approved by:	Kingston Educational Trust Board
Frequency of review:	At least every two years
Last review:	New trust wide policy
Next review due:	February 2025

Contents

1. Aims

Our trust and its schools aim to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law .

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

2. Legislation and guidance

This policy meets the requirements of:

- UK General Data Protection Regulation (UK GDPR) (the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020)
- Data Protection Act 2018 (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 the use of biometric data. It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

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

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.

Acronyms used in this policy:
DPA 2018: Data Protection Act 2018 (DPA 2018)
DPO: Data Protection Officer
UK GDPR: UK General Data Protection Regulation
ICO: Information Commissioner's Office

4. The data controller

The trust is the data controller for its schools and processes personal data relating to parents, pupils, staff, trustees, visitors and others.

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

5. Roles and responsibilities

This policy applies to **all staff** employed by the 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 Trust board

The trust board has overall responsibility for ensuring that the trust and our school 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 (this will also be shared and reviewed at its Buildings, Finance and Resources committee) and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the trust and its schools process, and for the ICO.

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

Our DPO is Zara Gallagher and is contactable via:

email dataprotection@kingstoneducationaltrust.org
telephone: 020 8465 6200

5.3 Executive Director and Head teacher

The head teacher in each school (and the Executive Director in respect of the Central Services Team) 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 trust's HR team of any changes to their personal data, such as a change of address;
- 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 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 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.

6. Data protection principles

The UK GDPR is based on data protection principles that our trust and its school 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 (data minimisation);
- 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 schools aim to comply with these key principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful basis' (legal reasons) to do so under data protection law:

- 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 (i.e the provision of education);
- 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 e.g. to protect someone's life;
- The data needs to be processed for the **legitimate interests** of the trust/its schools (where the processing is not for any tasks the trust/its schools perform 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent;**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law;**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for the establishment, exercise or defence of **legal claims;**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation;
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent;**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights;**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect personal data directly from individuals, we will set out the relevant information required by data protection law, this will usually be in a Privacy Notice.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will 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.

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised, subject to the requirements to retain certain data in accordance with the trust's Retention and Destruction schedule (copy to be published on the Data Protection Page of the Trust website).

8. Sharing personal data

Full and up to date details of who we share personal data with are set out in our Privacy Notices (copies are published on the Data Protection Page of the school/trust website or for staff in the Data Protection folder

in the Shared Drive). 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 that pupil or our staff or other 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 UK data protection law:
    - Ensure that the contract with the supplier or contractor covers the points required under the UK GDPR, 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 but not limited, 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, as long as personal data is sufficiently anonymised or consent has been provided.

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

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the trust/ its schools hold 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.

So that we can respond and locate the information required quickly it is helpful if requests are made in writing, using the school's Subject Access Request Form (available from the Data Protection Page of the schools' websites) and include at least:

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

If any member of staff receives a subject access request (whether in writing or a verbal request) they must immediately forward it/details to 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 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 below the age of 12 may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils aged 12 and above 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. A Pupil Consent Form is available from the Data Protection page of the school website.

9.3 Applications made on behalf of individuals by third parties

Any individual, including a child with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances we must have written evidence that the individual has authorised the person to make the application and the Data Protection Officer must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates. The Pupil Consent Form available from the Data Protection page of the school website may be adapted for this purpose.

9.4 Responding to subject access requests

When responding to requests, we:

- May ask for any further information reasonably required to locate the information;
- May ask the individual to provide 2 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/ consent 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.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s). We will not disclose information if for example it:

- Might cause serious harm to the physical or mental health of the pupil or another individual;
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, or where seeking consent would not be reasonable and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts or is given in court proceedings or contained in adoption or parental order records.

If we intend to apply any exemption to a request then we will usually explain which exemption is being applied and why.

All files must be reviewed by the Data Protection Officer before any disclosure takes place. Access will not be granted before this review has taken place.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

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 can seek to enforce their subject access right through the courts.

9.5 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 (usually provided in a Privacy Notice see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time;
- Ask us to rectify, erase or restrict processing of their personal data, 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, official authority or legitimate interests;
-
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- Be notified of a data breach (in certain circumstances);
- Make a complaint to the ICO;

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO (email:dataprotection@kingstoneducationaltrust.org). If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see their child's educational record

As an academy trust, there is no automatic parental right of access to the educational records our schools hold. Where parents, or those with parental responsibility, make a reasonable request for a copy of a document containing information regarding their child and that would be shared with them in the usual course of business in any event (such as assessment data, attendance or behavior records), these will be provided within 15 school days of receipt of a written request. Other requests for information will be dealt with as a Subject Access Request (see section 9) and must be immediately passed to the Data Protection Officer.

11. Biometric recognition systems

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

The Kingston Academy has, in the past, used a biometric recognition system in relation to cashless catering, but, as at the date of this policy, this system is not in use.

If pupils' biometric data is used within the trust at any time, as part of an automated biometric recognition system , 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 school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use a school's biometric systems. We will therefore provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can also withdraw consent, at any time, and in those circumstances we will make sure that any relevant data already captured is deleted.
As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

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

12. CCTV

Our schools use CCTV around their sites for the purpose of crime prevention and detection and for protecting the safety and wellbeing of pupils, staff and visitors (including at times to support behaviour management in school). We will adhere to the ICO's guidance for the use of CCTV and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are visible and there is signage throughout the site explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Facilities/Site Manager (or to the DPO if the enquiry relates to a data protection issue). **See also the separate CCTV policy.**

13. Photographs and videos

As part of our schools' activities, they may take photographs and record images of individuals within our schools. Photographs and videos taken of pupils and staff for a purpose that falls within the provision of education come under the public task purpose and consent is not required (such as the pupil/staff photographs used for identification purposes in the schools' management information systems or where for example a video is made as an element of the curriculum).

Where we use photographs or videos to promote a school/the trust or for another purpose which does not fall clearly within the public task/provision of education, we will obtain the consent of the individuals shown (including staff and trustees)/or their parents/carers (see below) before they are published.

As personal data about a child belongs to that child, we seek the consent of pupils where they are aged 12 or above, as this is the age where children are generally considered capable of providing informed consent for data processing. However, a pupil's ability to understand their rights will always be judged on a case-by-case basis.

For safeguarding reasons we also obtain consent from parents/carers of all pupils aged below 18.

Where we seek consent we will set out the intended uses of images and make it clear that consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete any photograph or video held and not distribute it further.

When we publish photographs and videos of pupils we will not include their full names in any accompanying text.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

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 school'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;
- 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 our school 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, 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

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

- Paper-based records that contain personal data are kept under lock and key when not in use;

- Papers containing confidential personal data must not be left unattended on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access;

- Access to school computers, laptops and other electronic devices is password protected. Staff and pupils are reminded not to share their passwords;

- All school laptops issued to staff are encrypted to prevent unauthorised access to any personal data on the hard drive if the laptop is lost or stolen. Data is not permitted to be removed from school using a USB device;

- When staff (or trustees) use a personal device to access personal data remotely, this should not be downloaded and stored on that device. Staff and trustees should ensure they log out when they have finished;

- 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).

16. Disposal of records

Personal data that is no longer needed will be disposed of securely (subject to retention requirements). 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/school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.
In the event of a suspected data breach, we will follow the procedure set out in the Appendix to this policy. When appropriate, we will report the data breach to the ICO within 72 hours.

18. Training

All staff and trustees/trust associates are provided with data protection guidelines as part of their induction process and regular updates/reminders.

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

The DPO is responsible for monitoring and reviewing this policy. This policy will be updated at least every two years or sooner if required to reflect statutory amendments.

Next review due: February 2025

Approved by Kingston Educational Trust Board
Date: 27 March 2023

Appendix: Breach Reporting Procedures

These procedures are based on the guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO) either by telephone or by email to: dataprotection@kingstoneducationaltrust.org .
- 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 head teacher and the chair of the Trust Board/Chair of the relevant local academy committee when a breach has occurred (unless the breach is minor and it is clear there is no risk to people's rights and freedoms).
- 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 these procedures).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. 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.

- 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 in the Breach Log for each school/the trust.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or by telephone without undue delay and in all cases 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 consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies;

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - Facts and cause;
    - Effects;
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored in the relevant Breach Log in the school or trust Google Drive.

Following any breach that is reported to the ICO the DPO, the Executive Director, Head teacher and (depending on the nature of the breach) the trust's Technology Strategic Lead will meet to review what happened and how it can be stopped from happening again and the effectiveness of the response. This meeting will happen as soon as reasonably possible following the breach.

Actions to minimise the impact of data breaches

The actions set out below may be taken to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The effectiveness of these actions will be reviewed and the actions developed and amended 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, as soon as they become aware of the error the sender must contact the DPO and 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.

- 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 and delete the information and not share, publish, save or replicate it in any way.