Cedars Manor School

Data Protection Policy – September 2025

Prepared by:	
Approved by:	*Full Governing body*
Signature of Chair of Governors:	
Status & review cycle	*Statutory Annual*
Date approved:	*November 2024*
Revised Update:	*September 2025*
Next Review Date:	*November 2027*

The Cedars Manor community believes that together, we will prepare each and every child for a bright future in an ever-changing world. We believe that by planting the seeds for a successful future our children, staff, parents and community can achieve educational excellence and shape the future through our 'B' values:

Safeguarding Team Contacts at Cedars Manor School

Role:	**Name and contact details:**
Designated Safeguarding Lead (DSL)	Kathy-Ann McClean Magda Bellis
Deputy DSL(s)	Emma Brice Julie Smeulders
Named safeguarding governor	Sameera Wazeri
Chair of Governors	Anthony Kent
School online safety Lead	Hayam Elsway
Designated teacher for Children in Care and children previously in care (CiC)	Kathy-Ann McClean
Senior Mental Health Lead	Magda Bellis
Mental Health Practioner	Adna Hooriyeh
Prevent Lead	Kathy-Ann McClean

Table of Contents

Article 8 (Protection and Preservation of Identity)

Every child has the right to an identity. Governments must respect and protect that right, and prevent the child's name, nationality, or family relationships from being changed unlawfully.

1. Aims

Our school is committed to ensuring that all personal data collected, stored, and processed about staff, pupils, parents, governors, visitors, and other individuals is handled in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, whether held digitally or in physical format, and to all processing activities carried out by the school or on its behalf by third parties.

2. Legislation and guidance

This policy is based on the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It is informed by guidance from the Information Commissioner's Office (ICO), including:

- The ICO's guidance on data protection in education
- The code of practice on subject access requests
- The code of practice for surveillance cameras and personal information

The policy also reflects the school's legal obligations under:

- Regulation 5 of the Education (Pupil Information) (England) Regulations 2005
- Safeguarding legislation (e.g. Keeping Children Safe in Education)
- Employment legislation
- The Freedom of Information Act 2000 (where applicable)

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.

TERM	DEFINITION
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › Health – physical or mental › Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

The school collects and processes personal data relating to pupils, parents and carers, staff, governors, contractors, volunteers, and visitors. As such, Cedars Manor School is a data controller under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The school is registered as a data controller with the Information Commissioner's Office (ICO) and renews this registration annually, or as otherwise legally required. Details of the school's registration, including our ICO registration number, can be found on the ICO's public register at www.ico.org.uk.

For queries regarding how the school processes personal data, or to exercise your data protection rights, please refer to the school's Data Protection Officer (DPO). Contact details are provided in Section 5.2 of this policy.

5. Roles and Responsibilities

This policy applies to all staff employed by the school, as well as to external organisations or individuals who process data on the school's behalf (known as *data processors*).

All individuals are expected to comply with this policy and relevant data protection legislation. Staff who do not comply may be subject to disciplinary action, in line with the school's disciplinary procedures.

Responsibilities are as follows:

- **Governing Body / Trustees**: Responsible for approving this policy and ensuring that the school has appropriate systems and policies in place to comply with data protection legislation.
- **Headteacher / Principal**: Has overall responsibility for ensuring that the school complies with data protection law and that staff understand their obligations. The Headteacher delegates day-to-day compliance tasks to the Data Protection Officer (DPO).
- **Data Protection Officer (DPO)**: The DPO monitors compliance, advises on the school's data protection obligations, provides guidance, supports training, and acts as a point of contact with the Information Commissioner's Office (ICO) and individuals exercising their data rights.
- The DPO is independent and reports directly to the governing body.
- **All Staff**: Are responsible for:
    - Handling personal data securely and in accordance with this policy
    - Completing any required data protection training
    - Reporting data breaches or suspected breaches without delay
    - Seeking guidance from the DPO when unsure about any data protection issue
- **External Data Processors**: Organisations or individuals working on behalf of the school (e.g. IT service providers, payroll processors) must:
    - Sign a data processing agreement
    - Only process personal data under the school's instruction
    - Implement appropriate security measures
    - Notify the school without delay of any data breaches

5.1 Governing Body

The Governing Body (or Trust Board, where applicable) has overall strategic responsibility for ensuring that the school complies with all relevant data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Governing Body is responsible for:

- Approving this Data Protection Policy and reviewing its effectiveness regularly

- Ensuring that the school has a named Data Protection Officer (DPO) in place
- Receiving reports from the DPO on data protection matters, including any significant risks or breaches
- Ensuring that appropriate resources and training are provided to support compliance

Day-to-day operational responsibility is delegated to the Headteacher and the school's Data Protection Officer.

5.2 Data Protection Officer (DPO)

The school has appointed a Data Protection Officer (DPO) in accordance with its obligations under the UK General Data Protection Regulation (UK GDPR).

The DPO is responsible for:

- Overseeing the implementation of this Data Protection Policy
- Monitoring the school's compliance with data protection legislation
- Advising on data protection impact assessments (DPIAs) and other compliance-related matters
- Developing and reviewing related data protection policies and guidance
- Acting as the first point of contact for data subjects (e.g. staff, parents, pupils) regarding their rights and the processing of their data
- Liaising with the Information Commissioner's Office (ICO) where necessary

The DPO reports directly to the Governing Body and provides an annual report on data protection activities, as well as advice and recommendations throughout the year.

The DPO operates independently and will not be dismissed or penalised for performing their data protection duties.

Our DPO is Alison Jones, who can be contacted via email at:

DPO@cedarsmanor.harrow.sch.uk

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

5.3 Headteacher

The Headteacher is responsible for ensuring that the school complies with data protection law on a day-to-day basis. Acting on behalf of the data controller (the school), the Headteacher:

- Oversees the implementation of data protection procedures across the school
- Ensures that all staff are aware of their responsibilities and receive appropriate training

- Supports the Data Protection Officer in their role and facilitates access to necessary resources
- Ensures that data protection impact assessments (DPIAs) are completed where required
- Oversees responses to subject access requests, data breaches, and other data rights requests, with support from the DPO
- Embeds data protection principles into school operations, systems, and decision-making

5.4 All Staff

All school staff have a responsibility to protect the personal data of pupils, colleagues, parents, and others in line with this policy and applicable data protection legislation.
Staff are responsible for:

- Collecting, storing, accessing, and processing personal data in accordance with this policy and the school's data handling procedures
- Informing the school promptly of any changes to their own personal data (e.g. address, contact details)
- Reporting any actual or suspected data breach immediately to the DPO or senior leadership

Staff must contact the Data Protection Officer in the following situations:

- If they have questions about how this policy should be applied
- If they are unsure whether they have a lawful basis for using personal data in a particular way
- If they need to:
    - Rely on or collect consent for data use
    - Draft or update a privacy notice
    - Respond to a data subject rights request (e.g. access, rectification, erasure)
    - Share personal data with a third party (e.g. a contractor, another school, or agency)
    - Transfer personal data outside the United Kingdom.
    - Review or enter into any data-sharing agreement or contract involving personal data
    - If they are planning a new project or activity that could affect the privacy rights of individuals (e.g. launching a new app, using biometric data, or introducing CCTV)
    - If they have any concerns that this policy is not being followed or that data is at risk.

6. Data Protection Principles

The UK General Data Protection Regulation (UK GDPR) establishes key principles that our school must follow when processing personal data. These principles require that personal data shall be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate data is erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Our school is committed to complying with these principles and has implemented policies, procedures, and controls to ensure that all personal data is handled appropriately and in line with legal requirements.

We also take responsibility for demonstrating our compliance with these principles at all times.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school 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 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

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

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

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

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

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit, and legitimate purposes. We will clearly inform individuals of these purposes at the time their data is collected.

If we intend to use personal data for any purpose other than those originally specified, we will inform the individuals affected prior to doing so and seek their consent where required.

Staff must only process personal data where it is necessary to fulfil their professional responsibilities.

When personal data is no longer required for the purposes for which it was collected, staff must ensure it is securely deleted or anonymised in accordance with the school's data retention and disposal policy.

8. Sharing Personal Data

We will not normally share personal data with third parties unless one of the following applies:

- There is a concern about a pupil or parent/carer that may put the safety of our staff or others at risk;
- We need to liaise with other agencies, in which case we will seek consent where appropriate before sharing;
- Our suppliers or contractors require data to provide services to staff or pupils, for example, IT providers. In such cases, we will:
  - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law;
  - Establish a written data sharing agreement with the supplier or contractor, either incorporated in the contract or as a standalone agreement, to ensure fair and lawful processing of any personal data shared;
  - Share only the data necessary for the supplier or contractor to carry out their service and any information needed to ensure their safety while working with us.

We will also share personal data with law enforcement and government agencies where we are legally required to do so, including but not limited to:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HM Revenue & Customs;
- In connection with legal proceedings;
- To satisfy our safeguarding obligations;
- For research and statistical purposes, provided that personal data is sufficiently anonymised or explicit consent has been obtained.

We may also share personal data with emergency services and local authorities to assist them in responding to emergency situations affecting our pupils or staff.

Where personal data is transferred to a country or territory outside the European Economic Area (EEA), we will ensure such transfers comply with data protection law and are subject to appropriate safeguards.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have the right to make a subject access request (SAR) to obtain information about the personal data the school holds about them. This includes the right to:

- Confirm whether their personal data is being processed;
- Access a copy of their personal data;
- Be informed of the purposes of the data processing;
- Know the categories of personal data concerned;
- Know who the data has been or will be shared with;
- Be informed how long the data will be stored, or if this is not possible, the criteria used to determine this period;
- Know the source of the data if it was not collected directly from the individual;
- Be informed if any automated decision-making, including profiling, is being applied to their data, and the significance and potential consequences of such processing.

Subject access requests should include:

- The name of the individual making the request;
- A correspondence address;
- Contact number and email address;
- Details of the information requested.

Any staff member who receives a subject access request must promptly forward it to the Data Protection Officer (DPO) without delay

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child and not to their parents or carers. For a parent or carer to make a subject access request on behalf of their child, the school must be satisfied that the child:

- Is unable to understand their rights and the implications of a subject access request; or
- Has given their explicit consent for the request.

Generally, children under the age of 12 are not considered mature enough to fully understand their rights and the consequences of a subject access request. Therefore, subject access requests made by parents or carers of pupils under 12 at our school will usually be granted without requiring the child's express permission.

However, this is not a blanket rule, and the child's ability to understand their rights will be assessed on a case-by-case basis, considering their age, maturity, and understanding.

9.3 Responding to Subject Access Requests

When responding to subject access requests, we will:

- Ask the individual to provide two forms of identification to verify their identity, where necessary;
- Contact the individual by phone or other means to confirm the authenticity of the request, if appropriate;
- Respond without undue delay and within one calendar month of receiving the request;
- Provide the requested information free of charge;
- Where a request is complex or numerous, inform the individual within one month that the response will take up to three calendar months, explaining the reasons for the extension.

We will not disclose personal data if doing so:

- Could cause serious harm to the physical or mental health of the pupil or another individual;
- Would reveal that a child is at risk of abuse, where disclosure would not be in the child's best interests;
- Is contained in adoption or parental order records;
- Has been provided to a court in proceedings concerning the child.

If a request is manifestly unfounded or excessive, particularly if it is repetitive or requests further copies of the same information, we may:

- Refuse to act on the request; or
- Charge a reasonable fee based on administrative costs.

In all cases where a request is refused or a fee charged, we will explain the reasons to the individual and inform them of their right to complain to the Information Commissioner's Office (ICO)

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see section 9.1) and the right to be informed about how we collect and use personal data (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where consent is the lawful basis for processing;
- Request rectification, erasure, or restriction of processing of their personal data, or object to processing in certain circumstances;
- Prevent the use of their personal data for direct marketing purposes;
- Challenge processing that has been justified on the basis of public interest;
- Request details of any agreements under which their personal data is transferred outside the European Economic Area (EEA);

- Object to decisions based solely on automated decision-making or profiling, where such decisions produce legal effects or similarly significant impacts;
- Prevent processing that is likely to cause damage or distress;
- Be notified of a personal data breach affecting them, where required by law;
- Make a complaint to the Information Commissioner's Office (ICO);
- Request that their personal data be transferred to another organisation in a structured, commonly used, and machine-readable format (data portability), where applicable.

Individuals wishing to exercise any of these rights should submit their request to the Data Protection Officer (DPO). Any staff member receiving such a request must forward it promptly to the DPO.

10. Parental Requests to See the Educational Record

Parents or individuals with parental responsibility have a legal right to free access to their child's educational record.

Upon receiving a written request, the school will provide access to the educational record within 15 school days.

Educational records include most information held about the pupil by the school.

11. CCTV

We use CCTV cameras in various locations around the school site to help ensure the safety and security of pupils, staff, visitors, and school property.

The use of CCTV is carried out in accordance with the Information Commissioner's Office (ICO) Code of Practice for Surveillance Cameras and Personal Information.

While we do not require individuals' consent to operate CCTV, we ensure that the presence of cameras is made clear by:

- Positioning cameras in visible locations;
- Displaying prominent signs informing individuals that CCTV is in operation.

Any enquiries or requests relating to the CCTV 'system' should be directed to the Premises Manager as first point of call.

12. Photographs and Videos

As part of school activities, we may take photographs and record videos of individuals within our school community.

We will obtain written consent from parents or carers before taking or using photographs and videos of their child for communication, marketing, or promotional purposes.

We will clearly explain to both parents/carers and pupils how the images will be used.

Possible uses include:

- Display within school premises, such as on notice boards, brochures, newsletters, and other printed materials;
- Use by external organisations, such as the school photographer or local newspapers;
- Publication on the school's official website or social media channels.

Consent may be refused or withdrawn at any time. If consent is withdrawn, we will delete the relevant images and cease further distribution.

When using photographs or videos in these ways, we will not include any additional personal information that could identify the child, in order to protect their privacy.

For more information on our use of images, please refer to our Child Protection and Safeguarding Policy.

13. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Cedars Manor School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Cedars Manor School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

14. Data Protection by Design and Default

We are committed to integrating data protection into all our data processing activities by implementing the following measures:

- Appointing a suitably qualified Data Protection Officer (DPO) and providing them with the necessary resources to perform their duties and maintain up-to-date expert knowledge;
- Ensuring that we only process personal data that is necessary for each specific purpose and always in accordance with the data protection principles set out in relevant data protection legislation (see section 6);
- Conducting Privacy Impact Assessments (PIAs) or Data Protection Impact Assessments (DPIAs) when our processing is likely to result in a high risk to the rights and freedoms of individuals, including when introducing new technologies. The DPO will provide guidance and oversight of this process;
- Embedding data protection considerations into all internal documentation, including this policy, related policies, and privacy notices;
- Providing regular data protection training to all staff, ensuring they understand their responsibilities under data protection law and this policy, and maintaining records of attendance;

- Conducting periodic reviews and audits to assess the effectiveness of our privacy measures and ensure ongoing compliance;
- Maintaining comprehensive records of our data processing activities, including:

    - Making available to data subjects the name and contact details of the school and the DPO, as well as information required by law about how we use and process their personal data (via privacy notices);
    - Keeping internal records detailing the types of personal data processed, the data subjects involved, purposes of processing, any third-party recipients, data storage methods, retention periods, and the security measures in place.

15. Data Security and Storage of Records

We are committed to protecting personal data by safeguarding it against unauthorised or unlawful access, alteration, processing, disclosure, and against accidental loss, destruction, or damage.
To achieve this, we implement the following measures:

- Paper-based records and portable electronic devices (e.g., laptops, hard drives) containing personal data are kept securely under lock and key when not in use;
- Confidential documents must never be left unattended on desks, tables, notice boards, or in any other areas accessible to unauthorized individuals;
- When personal data needs to be taken off-site, staff must sign it in and out via the school office to maintain a clear record of its movement;
- Access to school computers, laptops, and other electronic devices requires passwords of at least eight characters, incorporating letters and numbers. Staff and pupils are regularly reminded to update their passwords;
- All portable devices and removable media (e.g., laptops, USB drives) are protected with encryption software;
- Staff, pupils, and governors who store personal data on their personal devices are required to comply with the same security standards as for school-owned equipment, as outlined in our Online Safety Policy, ICT Policy, and Acceptable Use Agreement;
- Before sharing personal data with third parties, the school conducts due diligence and takes reasonable steps to ensure that the data will be stored securely and adequately protected (see section 8 for further details).

16. Disposal of Records

Personal data that is no longer required for the purposes for which it was collected,

or that is inaccurate or outdated and cannot be corrected, will be disposed of securely.

Disposal methods include shredding or incinerating paper records, and securely overwriting or deleting electronic files to ensure that personal data cannot be reconstructed or retrieved.

When using third-party services to dispose of records, the school will only appoint providers who can demonstrate sufficient guarantees of compliance with data protection legislation and ensure the secure destruction of data.

17. Personal Data Breaches

The school will take all reasonable steps to prevent personal data breaches and maintain the security of personal information.

In the unlikely event of a suspected data breach, the school will follow the procedure outlined in Appendix 1. Where required by law, we will report the breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.

Examples of personal data breaches relevant to the school context include, but are not limited to:

- The accidental publication of a non-anonymised dataset on the school website containing sensitive pupil information, such as exam results for pupils eligible for pupil premium;
- Safeguarding information being disclosed to an unauthorised person;
- The theft or loss of a school laptop containing unencrypted personal data about pupils.

18. Training

Data protection training will be provided to all staff as part of their ongoing professional development.

This training will be updated regularly to reflect changes in legislation, guidance, or school processes to ensure continued compliance and awareness.

19. Monitoring Arrangements

The Data Protection Officer (DPO) is responsible for monitoring and reviewing this policy to ensure it remains compliant with data protection laws and best practices.

This policy will be reviewed and updated as necessary in response to any legislative changes, including when the Data Protection Bill becomes law as the Data Protection Act 2018, or if any amendments affect the school's data protection practices.

Otherwise, the policy will be reviewed at least every two years and the updated version will be shared with the full Governing Body for approval.

20. Links with Other Policies

This data protection policy is linked to and should be read alongside the following policies:

- Freedom of Information Publication Scheme – Privacy Notice
- Online Safety Policy
- Acceptable Use of ICT Policy
- Child Protection and Safeguarding Policy

Appendix 1: Personal Data Breach Procedure

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

Immediate Actions

- Any staff member or data processor who discovers or causes a breach, or suspects one, must immediately notify the Data Protection Officer (DPO).
- The DPO will investigate the incident to determine if a breach has occurred. This involves checking if personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available when it should not have been
    - Made available to unauthorized persons
    - The DPO will promptly inform the Headteacher and Chair of Governors.

Containment and Assessment

- The DPO will work to contain and minimize the impact of the breach, with support from relevant staff or data processors.
- The DPO will assess the potential consequences based on the seriousness and likelihood of the breach's impact.
- The DPO will decide whether the breach must be reported to the ICO. This decision is made on a case-by-case basis considering if the breach is likely to negatively affect individuals' rights and freedoms, including risks such as:
    - Loss of control over data
    - Discrimination
    - Identity theft or fraud
    - Financial loss
    - Unauthorized reversal of pseudonymisation (e.g., key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage

If the risk to individuals' rights and freedoms is likely, the DPO must notify the ICO.

Documentation and Reporting

- The DPO will **document the decision** whether or not to report the breach, in case of future challenges by the ICO or affected individuals.
- If reporting is necessary, the DPO will submit a report to the ICO within 72 hours using the ICO's 'report a breach' webpage. The report will include:
    - A description of the nature of the breach, including categories and approximate number of individuals and data records involved (where possible)

    - The DPO's contact details
    - Likely consequences of the breach
    - Measures taken or planned to address the breach and mitigate its effects

- If full details are not yet available within 72 hours, the DPO will provide what is known, explain the delay, and submit the remaining information as soon as possible.

Informing Individuals and Third Parties

- If the breach poses a high risk to affected individuals, the DPO will inform them promptly in writing, including:

    - The DPO's contact details
    - A description of likely consequences
    - Measures taken or planned to mitigate adverse effects

- The DPO will also notify relevant third parties who can assist in mitigating risks, such as police, insurers, banks, or credit card companies.

Record Keeping and Review

- Every breach will be recorded, regardless of whether it is reported to the ICO. Each record will include:

    - Facts and cause of the breach
    - Its effects
    - Actions taken to contain it and prevent recurrence (e.g., improved processes or additional training)

- The DPO and Headteacher will meet as soon as reasonably possible to review the breach and determine further prevention measures.

Specific Actions for Data Breaches via Email (Sensitive or Special Category Data)

- If sensitive data is mistakenly sent via email to unauthorized recipients, the sender should attempt to recall the email immediately.
- Recipients who receive personal data in error must notify the sender and DPO immediately.
- If the sender cannot recall the email, the DPO will request assistance from the ICT department to recall it.
- If recall fails, the DPO will contact unauthorized recipients, explain the error, and request deletion of the data without sharing, publishing, saving, or copying it.
- The DPO will obtain written confirmation that recipients have complied.
- The DPO will search online to ensure the information has not been made public. If it has, the DPO will contact the publisher or website administrator to request removal.

Examples of Other Breach Scenarios

- Publishing named pupil premium intervention details on the school website.
- Sharing non-anonymized pupil exam results or staff pay information improperly.
- Theft or hacking of a school laptop containing unencrypted sensitive data.
- Hack of the school's cashless payment provider leading to stolen parental financial details.