



Name of Policy: Data Protection Policy

Policy Owner:	SLT
Type of Policy:	Statutory
Regulatory Body:	Department for Education / Independent Schools Inspectorate
Relevant Legislation/Guidance:	Data Protection Act 2018 UK General Data Protection Regulation (UK GDPR) Data (Use and Access) Act 2025 Information Commissioner's Office (ICO) Guidance Department for Education (DfE) Guidance
Last Reviewed By/Date:	Sep 2026
Last Approved By/Date:	Sep 2026
Next Review Due:	Sep 2027
This Version Published:	Sep 2026 (Website and Policy Folder)
Circulation:	✓All Staff & Governors ✓Inspection Portal ✓School Website
Linked Policies:	Information & Records Retention Policy; Privacy notices; Pupil IT Acceptable Use Policy; Staff IT Acceptable Use Policy; ICT Acceptable Use Policy for Parents; Online Safety Policy; CCTV Policy.

Data Protection Policy

Table of Contents

1. Aims
2. Legislation and Guidance
3. Definitions
4. The Data Controller
5. Roles and Responsibilities
6. Data Protection Principles
7. Collecting Personal Data
8. Limitation, Minimisation, and Accuracy
9. Sharing Personal Data
10. Subject Access Requests and Other Rights of Individuals
11. Parental Requests to See the Educational Record
12. CCTV and Surveillance
13. Photographs and Videos
14. Artificial Intelligence (AI) and Generative Chatbots
15. Data Protection by Design and Default
16. Data Security and Storage of Records
17. Disposal of Records
18. Personal Data Breaches
19. Training
20. Complaints
21. Record Keeping and Review
22. Links with Other Policies
23. Appendix 1: Personal Data Breach Procedure

1. Aims

St Margaret's School aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, 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 held in paper or electronic format, and covers all members of the school community.

2. Legislation and Guidance

This policy meets the requirements of the following statutory and regulatory frameworks:

- The UK General Data Protection Regulation (UK GDPR), which incorporates the EU GDPR into UK legislation as amended by *The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020*;

- The Data Protection Act 2018 (DPA 2018);
- The Data (Use and Access) Act 2025 (DUAA 2025);
- The Protection of Freedoms Act 2012 (which governs the school's use of biometric data).

It is based on regulatory guidance published by the Information Commissioner's Office (ICO) on the UK GDPR, the ICO's *Surveillance Camera Code of Practice*, and guidance from the Department for Education (DfE) on *Generative Artificial Intelligence in Education*.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This includes names (including initials), identification numbers, location data, and online identifiers (e.g. usernames, IP addresses). It also covers physical, physiological, genetic, mental, economic, cultural, or social factors.
Special categories of personal data	Personal data which is highly sensitive and requires enhanced protection [58]. This includes information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (where used for identification), health (physical or mental), sex life, or sexual orientation [59].
Processing	Any operation performed on personal data, whether automated or manual. This includes collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying.
Data subject	The identified or identifiable living individual whose personal data is being held or processed.
Data controller	The 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 security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

St Margaret's School processes personal data relating to parents, carers, pupils, staff, governors, visitors, and others, and is therefore registered as a **data controller** with the Information Commissioner's Office (ICO).

The School maintains its registration and has paid its statutory data protection fee to the ICO, as legally required.

5. Roles and Responsibilities

This policy applies to all staff employed by St Margaret's School, and to external organisations or individuals working on our behalf. Staff who fail to comply with this policy may face disciplinary action up to and including dismissal.

5.1 Governing Board

The Governing Board has overall responsibility for ensuring that St Margaret's School complies with all relevant UK data protection obligations.

5.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the School's compliance with data protection law, and developing related guidelines.

The DPO acts as the primary point of contact for the ICO and for individuals whose data the School processes. The DPO provides an annual report of their activities directly to the Governing Board and delivers advice and recommendations on school data protection issues.

Our Data Protection Officer is **Matt Brown**, who is contactable via email at mbrown@st-margarets.co.uk.

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis, ensuring operational compliance with data protection policies.

5.4 All Staff

All members of staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy;
- Informing the School of any changes to their personal data, such as a change of address;
- Contacting the DPO immediately in the following circumstances:
 - If they have any questions about the operation of this policy, data protection law, data retention, or security;
 - If they have concerns that this policy is not being followed;
 - If they are unsure whether they have a lawful basis to use personal data in a particular way;
 - If they need to rely on or capture consent, draft a privacy notice, deal with data subject rights, or transfer personal data outside the United Kingdom;
 - If there has been a suspected or actual data breach;
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
 - If they require assistance with third-party contracts or data sharing agreements.

6. Data Protection Principles

The UK General Data Protection Regulation is based on core principles that St Margaret's School must strictly adhere to. 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 those purposes;
- 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 manner that ensures appropriate security.

7. Collecting Personal Data

7.1 Lawfulness, Fairness, and Transparency

The School will only process personal data where it has established at least one of the six lawful bases (legal reasons) under data protection law:

1. **Contractual Necessity:** The processing is necessary to fulfil a contract with the individual, or to take specific pre-contractual steps requested by them.
2. **Legal Obligation:** The processing is necessary for the School to comply with a legal or statutory obligation.
3. **Vital Interests:** The processing is necessary to protect the life of the data subject or another individual.
4. **Public Task / Public Interest:** The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller [67]. (Note: As an independent school, this basis is applied primarily where the School is exercising specific statutory functions, such as safeguarding or pupil registration).
5. **Legitimate Interests:** The processing is necessary for the legitimate interests of the School or a third party, provided these are not overridden by the individual's fundamental rights and freedoms.
6. **Consent:** The individual (or their parent/carer when appropriate) has freely given clear, unambiguous consent for their data to be processed for a specific purpose.

7.2 Processing Special Category Personal Data

For special category personal data, we will also meet at least one of the special category conditions for processing:

- The individual (or their parent/carer when appropriate) has given explicit consent;
- The processing is necessary to perform obligations or exercise rights in relation to employment, social security, or social protection law;
- The processing is necessary to protect the vital interests of an individual who is physically or legally incapable of giving consent;
- The data has been made manifestly public by the individual;
- The processing is necessary for the establishment, exercise, or defence of legal claims;
- The processing is necessary for reasons of substantial public interest as defined in UK legislation (such as statutory safeguarding);
- The processing is necessary for health or social care purposes, conducted by or under the direction of a health or social work professional subject to professional confidentiality;
- The processing is necessary for public health reasons, conducted by or under the direction of a health professional subject to confidentiality;
- The processing is necessary for archiving, scientific, historical research, or statistical purposes in the public interest.

7.3 Processing Criminal Offence Data

For criminal offence data, we will meet both a lawful basis and an approved statutory condition under the Data Protection Act 2018. These conditions include explicit consent, vital interests, data made manifestly public, legal proceedings/advice, or reasons of substantial public interest.

Whenever we collect personal data directly from individuals, we will provide them with a compliant Privacy Notice. We will ensure we do not handle data in ways that individuals would not reasonably expect, or in ways which have unjustified adverse effects.

8. Limitation, Minimisation, and Accuracy

The School will only collect personal data for specified, explicit, and legitimate reasons, explaining these clearly to individuals at the point of collection. Staff must only process personal data where it is strictly necessary to perform their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased without delay. When personal data is no longer required, staff must ensure it is safely deleted or anonymised in accordance with the School's *Information & Records Retention Policy*.

9. Sharing Personal Data

The School will not normally share personal data with external parties without consent. However, we are permitted and required to do so under specific circumstances, including:

- Where there is an issue with a pupil or parent/carer that puts the safety of our staff or pupils at risk;
- Liaising with other statutory agencies (such as local safeguarding partners, children's social care, or health professionals) where safeguarding or student welfare duties apply;
- Sharing with law enforcement and government bodies (such as the DfE and local authorities) where we are legally required to do so;
- Sharing with emergency services to respond to an active emergency affecting pupils or staff;
- Sharing with suppliers or contractors (such as IT and EdTech companies) to enable us to provide educational or administrative services.
- When sharing data with suppliers or contractors, the School will:
 - Carry out robust due diligence to ensure they provide sufficient guarantees under UK data protection law;
 - Establish a legally binding contract (Data Processing Agreement) to govern the fair and secure processing of data;
 - Only share the minimum data necessary for the contractor to perform their specified service.

10. Subject Access Requests and Other Rights of Individuals

10.1 Subject Access Requests (SARs)

Individuals have a statutory right to make a Subject Access Request to gain access to personal information the School holds about them. This includes:

- Confirmation that their personal data is being processed;
- Access to a copy of their personal data;
- The purposes of the processing and the categories of data concerned;
- Details of third-party recipients with whom the data has been or will be shared;
- The retention period or the criteria used to determine it;
- The existence of the rights to request rectification, erasure, restriction, or to object to processing;
- The right to lodge a complaint with the ICO;
- The source of the data, if not collected directly from the individual;
- The existence of any automated decision-making or profiling;
- The safeguards in place if data is transferred internationally.

Subject Access Requests can be submitted in any form (including verbally). However, to expedite responses, the School encourages requests to be made in writing to the DPO, providing the requester's name, correspondence address, contact details, and a clear description of the information sought. Staff who receive a SAR in any form must forward it to the DPO immediately.

10.2 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 SAR on behalf of a child, the child must either be unable to understand their rights, or have given their express consent to the request.

- **Children below the age of 12:** Children in this age group are generally not regarded as mature enough to understand their rights and the implications of a SAR. Therefore, most SARs submitted by parents or carers of pupils under 12 may be granted without the pupil's express permission.
- **Children aged 12 and above:** Pupils in this age group are generally presumed mature enough to understand their rights and the implications of a SAR. Therefore, most SARs submitted by parents or carers of pupils aged 12 or over will require the express written permission of the pupil before data can be released.

Every request will be evaluated on a case-by-case basis, and a pupil's actual capacity to understand their rights will always be assessed individually.

10.3 Responding to Subject Access Requests

When responding to a Subject Access Request, the School:

- May request two forms of identification from the requester;
- May contact the individual to verify the authenticity of the request;
- Will respond without delay and within one calendar month of receipt;
- Will provide the information free of charge;
- May extend the response period to up to three months if the request is highly complex or numerous, notifying the individual within the first month and explaining the reason for the delay.

Vexatious or Excessive Requests: In accordance with the *Data (Use and Access) Act 2025*, where a request is determined to be vexatious or excessive (taking into account its repetitive nature, intent, and disproportionate burden), the School may refuse to act on the request, or charge a reasonable administrative fee. If the School refuses a request, we will write to the individual within one month explaining our reasons and advising them of their right to complain to the ICO or seek a court remedy.

Withholding Information: The School may withhold certain information if releasing it:

- Might 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, and disclosure would not be in their best interests;
- Would reveal another person's personal data without their consent, where it is not reasonable to do so and the data cannot be anonymised;
- Is exempt under the DPA 2018 (e.g. records subject to legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts).

10.4 Other Data Protection Rights of the Individual

In addition to the right of access, individuals have the right to:

- Withdraw consent to processing at any time;
- Request the rectification, erasure, or restriction of their personal data (in certain circumstances);
- Object to processing justified by public task, official authority, or legitimate interests;
- Prevent the use of their data for direct marketing;
- Challenge decisions based solely on automated decision-making or profiling;
- Be notified of a high-risk data breach;
- Request data portability in a structured, commonly used, and machine-readable format;
- Lodge a complaint with the School or directly with the ICO.

11. Parental Requests to See the Educational Record

As an independent school, there is no automatic statutory right under the *Education (Pupil Information) (England) Regulations 2005* for parents to access their child's educational record. However, in the interest of partnership and transparency, St Margaret's School chosen to provide parents with access to these records voluntarily.

11.1 Making a Request

- Requests must be submitted in writing to the Headteacher;
- The School will respond to requests within 15 school days during term time;
- We do not charge any fee for providing access to or copies of the educational record.

11.2 Record Contents and Exceptions

The educational record typically includes academic reports, progress assessments, attendance records, and records of significant educational incidents.

The School may withhold information from the educational record if releasing it might cause serious physical or mental harm to the pupil or another individual, would reveal unannounced exam marks, or contains the personal data of third parties who have not consented.

12. CCTV and Surveillance

St Margaret's School uses CCTV in various locations around the school site to maintain a safe and secure environment for pupils, staff, and visitors.

The system is operated in strict compliance with the ICO's Surveillance Camera Guidance and data protection principles. Security cameras are highly visible, and prominent signage is displayed across the premises explaining that CCTV is in use.

Any enquiries regarding the CCTV system, data storage, or footage access requests must be directed to Matt Brown, DPO.

13. Photographs and Videos

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

- **Written Parental Consent:** We will obtain prior written consent from parents/carers for photographs and videos of their child to be taken and used for school communications, marketing, and promotional materials;
- **Consent Withdrawal:** Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and cease its distribution;
- **Identification Protection:** When publishing photographs and videos (on notice boards, newsletters, or online), we will not accompany them with any other identifying personal details of the child (such as full names) to protect their identity;
- **Personal Use by Parents:** Photographs or videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, for safeguarding reasons, we request that parents do not share images featuring other pupils on public social media platforms unless they have obtained the express agreement of those pupils' parents.

14. Artificial Intelligence (AI) and Generative Chatbots

St Margaret's School recognises that generative Artificial Intelligence (AI) systems (such as ChatGPT and Gemini) offer innovative educational opportunities but also present substantial risks to data protection and information security.

- **Prohibition on Sensitive Data Entry:** To protect the privacy rights of our community, no student, staff member, governor, or contractor is permitted to enter any personal, confidential, or sensitive special category data into unauthorised generative AI systems;
- **Data Breach Classification:** Entering personal or sensitive data into an unauthorised AI chatbot will be treated by the School as an official personal data breach. Such incidents will trigger the personal data breach procedure outlined in Appendix 1 and must be reported to the DPO immediately.

15. Data Protection by Design and Default

The School implements technical and organisational measures to integrate data protection into all processing activities. This includes:

- Ensuring the DPO is suitably qualified and provided with the resources and independence necessary to maintain their expert knowledge;

- Adhering strictly to data minimisation, processing only the data necessary for each specific purpose;
- Completing a Data Protection Impact Assessment (DPIA) before introducing new technologies or processing activities that present a high risk to the rights and freedoms of individuals (guided by the DPO);
- Regularly training all staff on UK data protection law and School policies, maintaining an official record of training attendance;
- Conducting regular internal audits and reviews to test our privacy and security measures;
- Ensuring appropriate safeguards are in place for any international data transfers;
- Maintaining a comprehensive Record of Processing Activities (ROPA), documenting data types, categories of data subjects, purposes of processing, retention periods, and technical security measures.

16. Data Security and Storage of Records

The School implements robust security measures to protect personal data from unauthorised access, alteration, disclosure, accidental loss, damage, or destruction.

- **Physical Security:** Paper-based records containing personal data are kept under lock and key. All laptops are password protected. Sensitive papers must never be left unattended on desks or in staffrooms where there is general access;
- **Digital Security and Passwords:** Access to all school networks, computers, and devices is restricted. In line with National Cyber Security Centre (NCSC) best practices, passwords must be strong, unique, and follow the three random words guidance (aiming for a minimum of 12 characters). Staff and pupils are strictly prohibited from reusing passwords from other systems;
- **Personal Devices:** Staff, pupils, or governors who access school systems or store school-related personal data on personal devices (BYOD) are contractually bound to implement the same security procedures as school-owned equipment, in accordance with the *Staff and Pupil Acceptable Use Policies*;
- **Contracts:** All third parties sharing or handling school personal data must undergo robust due diligence and sign legally binding data protection clauses.

17. Disposal of Records

Personal data that is no longer required, or has become inaccurate/out-of-date and cannot be corrected, will be disposed of securely.

- Paper records containing personal data will be shredded or incinerated;
- Electronic files will be overwritten or securely deleted from all systems and backups;
- Where the School contracts a third-party disposal service, we will require written guarantees and certificates of destruction confirming complete compliance with UK data protection standards.

18. Personal Data Breaches

St Margaret's School makes all reasonable endeavours to prevent personal data breaches. In the event of a suspected or actual data breach, the School will immediately activate the Personal Data Breach Procedure outlined in Appendix 1.

Where a breach presents a risk to the rights and freedoms of individuals, the DPO will report the breach to the ICO within 72 hours of the School becoming aware of it. Such breaches in a school context may include:

- Unencrypted personal data or safeguarding files being shared with or accessed by unauthorised persons;
- Accidental publication of non-anonymised pupil premium or exam data on the school website;

- Theft or loss of a school device containing non-encrypted personal information.

19. Training

All staff and governors are provided with data protection training as part of their induction process. Ongoing data protection training forms a mandatory part of continuing professional development (CPD), especially following changes to UK legislation, regulatory guidance, or School processes.

20. Complaints

If you believe that the School has not processed your personal data (or the data of a child you have parental responsibility for) in accordance with UK legislation, you have the right to lodge a complaint with us.

Complaints may relate to the School's response to a SAR, data security measures, or data collection practices.

20.1 Submission Methods

Complaints should be directed to:

- **Email:** Matt Brown, Data Protection Officer, at mbrown@st-margarets.co.uk;
- **Phone:** Contacting the School Office;
- **Post:** In writing to the Headteacher at St Margaret's School, 18 Kidderpore Gardens, London, NW3 7SR.

Complainants do not need to use formal legal terms or cite specific sections of data protection legislation to raise a complaint.

20.2 How We Handle Complaints

- **Acknowledgment:** We will acknowledge receipt of your data protection complaint within 5 school days during term time (ensuring a prompt and professional response);
- **Investigation:** The DPO will investigate the complaint thoroughly and fairly, reviewing all relevant facts, interviewing staff, and checking School procedures;
- **Updates:** We will keep the complainant updated on our progress and explain any unavoidable delays;
- **Outcome:** We will write to the complainant as soon as possible with the outcome of our investigation, detailing our findings and any actions taken as a result.

20.3 Escalation to the ICO

If you remain dissatisfied with how the School has handled your complaint, you have the right to lodge a formal complaint with the Information Commissioner's Office (ICO).

- **Website:** <https://ico.org.uk/make-a-complaint/>
- **Telephone:** 0303 123 1113 [103]
- **Post:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

21. Record Keeping and Review

The DPO will maintain a secure, central register of all data protection complaints received, recording the date of receipt, acknowledgment, notes of all investigations, and the final outcome. Records will be retained in accordance with the School's *Information & Records Retention Policy*.

Following the resolution of any complaint, the DPO and Headteacher will review the incident to identify areas for system improvement and staff training.

This policy will be reviewed by the DPO and approved by the Governing Board annually.

22. Links with Other Policies

This Data Protection Policy is linked directly to our:

- Information & Records Retention Policy;
- School Privacy Notices (Parents, Pupils, and Staff);
- Pupil IT Acceptable Use Policy;
- Staff IT Acceptable Use Policy;
- IT Acceptable Use Policy for Parents;
- Online Safety Policy;
- CCTV Policy.

Appendix 1:

Personal Data Breach Procedure

This procedure is based on the statutory guidelines and self-assessment tools published by the Information Commissioner's Office (ICO).

1. Initial Notification and Investigation

- **Immediate Notification:** Any member of staff, governor, volunteer, or contractor who discovers or causes a personal data breach or suspected breach must notify the DPO via email immediately.
- **DPO Assessment:** The DPO will immediately investigate the report to determine if a breach has occurred [106]. They will assess whether data has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed, or made available to unauthorised individuals.
- **Cooperation:** All staff, governors, and contractors are required to cooperate fully with the DPO's investigation. The investigation is a compliance exercise and will not be treated as a disciplinary investigation.
- **Leadership Alert:** If a breach has occurred, or is highly likely to have occurred, the DPO will immediately alert the Headteacher and the Chair of Governors.

2. Containment and Mitigation

- The DPO will make all reasonable efforts to contain the breach and minimise its impact [107].
- Relevant staff or data processors must assist the DPO immediately [107]. The DPO will seek urgent external technical advice (e.g. from the ICT department or external IT providers) when necessary to secure systems.
- The DPO will formally assess the potential consequences of the breach, implementing and reviewing mitigation measures.

3. Assessing and Reporting to the ICO

- **Risk Assessment:** The DPO will use the ICO's self-assessment tool to determine whether the breach must be reported to the ICO and to the individuals affected.
- **Decision Log:** The DPO will document all decisions and rationale (whether reporting or not) to maintain an audit trail for the ICO. Logs will be stored securely on the School's network.
- **72-Hour Deadline:** Where a report is required, the DPO will notify the ICO via its website or breach report line (0303 123 1113) **within 72 hours** of the School becoming aware of the breach.
- **Report Contents:** The notification will include a description of the nature of the breach, the categories and approximate number of data subjects and records affected, the DPO's contact details, likely consequences, and mitigation measures. If full details are not yet known, the DPO will submit a phased report explaining the delay.

4. Notifying Affected Individuals

- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will notify those affected in writing without undue delay.
- The written notice will be in clear and plain language, describing the nature of the breach, the DPO's contact details, likely consequences, and measures taken to mitigate the risk.
- The DPO will consider whether notifying relevant third parties (such as the police, insurers, or banks) would help mitigate the loss.

5. Evaluation and Prevention

- Every breach (regardless of whether it is reported to the ICO) will be formally documented by the DPO, recording the facts, causes, effects, and containment actions.
- The DPO and Headteacher will meet as soon as reasonably possible following a breach to review the incident and establish preventative measures.
- They will meet regularly to assess trends and patterns in recorded breaches to proactively reduce future risks.

6. Specific Mitigation Actions (Examples)

A. Sensitive Safeguarding or Special Category Information Disclosed via Email

- The sender must attempt to recall the email immediately upon becoming aware of the error.
- Any staff member who receives school personal data in error must notify the sender and the DPO immediately.
- If a recall is unsuccessful, the DPO will instruct the ICT department to attempt to recall the email from external recipients' mail servers and purge it from the School's email system.
- If the email cannot be confirmed as deleted, the DPO will contact the recipient, explain the error, and obtain a written confirmation that they have deleted the email and will not share, save, or replicate the data.
- The DPO will conduct web searches to verify the information has not been published; if it has, they will contact the site host for immediate removal.
- If safeguarding information is compromised, the DPO will inform the Designated Safeguarding Lead (DSL) and determine whether a report is required to the local safeguarding partners.

B. Loss or Theft of a School Device

- The staff member must report the loss of any school laptop, phone, or tablet to the DPO and ICT department immediately.
- The ICT department will immediately initiate a remote wipe of the device.
- If the device was unencrypted and contained personal data, the DPO will treat this as a high-risk data breach and initiate immediate ICO and data subject notifications.