HOPEBRIGHT
SCHOOL

Data Protection Policy

Reviewed: September 2026

Review Date: September 2027

HOPEBRIGHT
SCHOOL

Data Protection Policy

Contents

Data Protection Policy (inc. Data Retention Schedule)

Aligned with UK GDPR, DPA 2018, Ofsted & ISI Requirements (2026)

Reviewed: September 2026

Next Review Date: September 2027

1. Purpose & Scope

Hopebright School is committed to full compliance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and associated statutory guidance, including updates reflecting evolving digital, safeguarding, and cyber security risks in education settings.

This policy ensures that personal data is:

- Processed **lawfully, fairly, and transparently**
- Used in line with **education, safeguarding, and regulatory duties**
- Protected against **loss, misuse, unauthorised access, or disclosure**
- Managed in a way that supports **Ofsted and ISI expectations for leadership, safeguarding, and record-keeping**

The School is registered with the **Information Commissioner's Office (ICO)** as a Data Controller.

This policy also supports compliance with:

- **Keeping Children Safe in Education (KCSIE 2025/26)**
- **Education (Student Information) (England) Regulations 2005**
- **ISI Regulatory Requirements (2025/26 Framework expectations)**
- Ofsted inspection criteria relating to **leadership, safeguarding effectiveness, and governance**

2. Definitions

(unchanged core definitions, with 2026 enhancement)

Personal Data: Any information relating to an identifiable individual.

Special Category Data: Includes health, safeguarding, ethnicity, religion, biometric data, sexual orientation, and genetic data.

Criminal Offence Data: Includes allegations, proceedings, convictions, and DBS-related safeguarding data.

Data Controller: Hopebright School.

Data Processor: Any third party processing data on behalf of the School (e.g. MIS providers, cloud systems, payroll services).

Cloud Service Providers: Approved third-party digital platforms used for storing or processing data (subject to GDPR-compliant contracts and UK/EU data hosting assurances).

3. Roles and Responsibilities

Board of Directors

Responsible for:

- Strategic oversight of data protection compliance
- Ensuring GDPR is embedded into governance
- Reviewing data breach trends and cyber risk

Data Protection Officer (DPO)

Chief Operations Officer

Email:

Responsible for:

- UK GDPR compliance oversight
- Advising leadership and governors
- Managing Data Protection Impact Assessments (DPIAs)
- Acting as ICO liaison
- Monitoring data breaches and cyber risks
- Ensuring staff training compliance

All Staff

Staff must:

- Handle data securely and lawfully
- Use only approved systems
- Avoid personal device use for school data unless authorised and encrypted
- Report breaches immediately
- Follow safeguarding-linked data handling procedures

4. Data Protection Principles

The School complies with Article 5 UK GDPR principles:

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability (documented compliance evidence required for Ofsted/ISI inspection readiness)

5. Lawful Processing

Processing is carried out under one or more lawful bases:

- Consent (where required and documented)
- Contract
- Legal obligation
- Vital interests
- Public task (education provision)
- Legitimate interests (balanced and risk-assessed)

Enhanced 2026 requirement:

All new digital systems and AI-enabled tools must undergo a **DPIA before deployment**.

6. Special Category & Criminal Offence Data

Hopebright School processes **Special Category Data** and **Criminal Offence Data** only where necessary, proportionate, and in strict compliance with **UK GDPR Articles 9 and 10**, the **Data Protection Act 2018**, and safeguarding obligations under **Keeping Children Safe in Education (KCSIE 2025/26)**.

Given the sensitive nature of this information, the School applies **enhanced governance controls, restricted access protocols, and heightened security measures**.

Categories of Sensitive Data Processed

Special Category Data includes:

- Child protection and safeguarding records
- Special Educational Needs (SEN) information
- Physical and mental health information
- Medical care plans and medication records
- Ethnicity and cultural background data (where recorded for statutory purposes)
- Religious belief information (where relevant and disclosed)
- Biometric data (where used for identification systems, if applicable)

Criminal Offence Data includes:

- DBS (Disclosure and Barring Service) checks and outcomes
- Allegations involving staff or pupils
- Records of safeguarding investigations
- Police or statutory authority disclosures
- Outcomes of disciplinary procedures involving safeguarding risk

Lawful Basis and Safeguarding Justification

Processing is undertaken only where:

- There is a **legal obligation** (e.g. safeguarding duties under KCSIE)
- Processing is necessary for **substantial public interest (education and safeguarding functions)**
- It is required to protect **vital interests of a child or vulnerable individual**
- There is explicit lawful authority under Schedule 1 of the Data Protection Act 2018

Access Controls and Security Restrictions

Access to Special Category and Criminal Offence Data is strictly controlled:

- Restricted to **Designated Safeguarding Lead (DSL)** and **Deputy DSLs**
- Limited access for **Senior Leadership Team (SLT)** on a strictly need-to-know basis
- Access logs are maintained and subject to audit
- Role-based permissions enforced within digital systems (RBAC)

Staff outside authorised roles:

- Must not access safeguarding or sensitive records
- Must not store copies of such data locally or on personal devices
- Must immediately report any accidental access or disclosure

Handling and Storage Requirements

Sensitive data is:

- Stored in **secure safeguarding systems or restricted MIS modules**
- Protected by encryption both in transit and at rest
- Kept separate from general pupil records where appropriate
- Never stored on unsecured drives, personal emails, or removable media

Paper records:

- Stored in locked safeguarding cabinets
- Access logged and restricted to authorised personnel only

Retention and Review

Special Category and Criminal Offence Data is retained in line with:

- KCSIE safeguarding expectations
- Legal limitation periods
- ICO guidance on necessity and proportionality

Records are:

- Regularly reviewed for continued necessity
- Retained securely where safeguarding relevance persists
- Never deleted where safeguarding risk or legal obligation remains

7. Individual Rights

Hopebright School fully recognises and upholds the rights of individuals under the UK General Data Protection Regulation (UK GDPR)**.** The School ensures that all rights requests are handled lawfully, transparently, and within statutory timescales, with safeguarding considerations prioritised where applicable.

Rights of Individuals

Individuals (including pupils, parents, staff, and third parties where applicable) have the following rights:

Right to be informed

- Clear privacy notices are provided explaining how data is collected and used
- Information is presented in accessible language appropriate to the audience

Right of access (Subject Access Requests – SARs)

- Individuals can request copies of their personal data held by the School

Right to rectification

- Inaccurate or incomplete data must be corrected without undue delay

Right to erasure

- Applies only where no overriding legal, safeguarding, or statutory requirement exists
- May be limited in education and safeguarding contexts

Right to restrict processing

- Individuals may request limitation of how data is used in certain circumstances

Right to object

- Individuals may object to processing based on legitimate interests or public task (where applicable)

Right to data portability

- Applies to data provided directly by the individual where processing is based on consent or contract

Rights relating to automated decision-making

- Individuals have protection from decisions made solely by automated processes where such decisions have legal or significant effects

Subject Access Requests (SARs)

The School manages SARs in accordance with UK GDPR requirements and ICO guidance.

Response Timescale

- All SARs are responded to within **1 calendar month**

Identity Verification

- The School will require sufficient proof of identity before releasing any personal data
- Requests made on behalf of others must include appropriate authorisation

Extensions

- Complex or multiple requests may be extended by up to **2 additional months**
- The requester will be informed of the extension and reasons for delay

Exemptions

The School may lawfully withhold or redact information where:

- Disclosure would prejudice safeguarding of a child
- Third-party data rights would be infringed
- Legal professional privilege applies
- Disclosure is restricted under education or safeguarding law

All decisions to redact or refuse data are:

- Documented
- Approved by the DPO
- Subject to review if challenged

8. Data Security

Hopebright School maintains a **robust, layered security framework** designed to meet and exceed expectations under UK GDPR, ICO guidance, **Ofsted safeguarding governance expectations**, and **ISI inspection standards**, including current UK government cyber resilience guidance for education providers.

The School adopts a **"defence in depth" approach**, combining physical, technical, and organisational controls.

Physical Security Controls

To protect paper-based and on-site records, the School ensures:

- Secure, lockable storage for all confidential and sensitive records
- Restricted access to staff-only areas
- Visitor access controls and sign-in procedures
- Clear desk policy in all administrative and safeguarding areas
- Secure disposal of confidential waste via shredding or approved destruction services

Digital Security Controls (Cyber Resilience Framework)

The School implements strong technical safeguards, including:

Authentication and Access Control

- Multi-factor authentication (MFA) required for all core systems
- Role-based access control (RBAC) limiting access to necessity
- Unique user accounts (no shared credentials)
- Immediate deactivation of accounts upon staff departure

Data Protection and Encryption

- Encryption of all portable devices (laptops, tablets, USB storage where permitted)
- Encryption of data in transit and at rest across systems
- Secure cloud hosting using UK GDPR-compliant providers where possible

System Security

- Regular patching and software updates
- Firewall protection and intrusion detection systems (where applicable)
- Monitoring of suspicious login activity and alerts
- Controlled access to administrative systems

Password Management

- Strong password requirements enforced
- Regular password updates in line with cyber security guidance
- Prevention of password reuse across systems

Approved Systems and Cloud Usage

- Only **School-approved platforms and systems** may be used for processing personal data
- All third-party systems must undergo:
    - Data Protection Impact Assessment (DPIA)

- Supplier due diligence checks
- Contractual UK GDPR compliance review

Unapproved applications or “shadow IT” systems are strictly prohibited.

Device Security and Usage

School Devices

- School-issued devices must be used for handling personal data
- Devices must remain encrypted and password protected at all times
- Automatic screen locking enabled

Personal Devices

- Use of personal devices is **not permitted unless explicitly authorised**
- Where authorised, additional safeguards apply (e.g. encryption, secure access methods)

Loss or Theft Procedures

In the event of device loss:

- Immediate reporting to IT and DPO is required
- Remote wipe functionality will be activated where available
- Risk assessment conducted to determine breach notification requirements

Remote Access and Working

Where remote access is permitted:

- Secure VPN or approved remote access tools must be used
- Public or unsecured Wi-Fi must not be used without protection
- No local storage of pupil or staff data is permitted

Monitoring and Continuous Improvement

The School:

- Regularly reviews cyber security controls
- Conducts periodic vulnerability assessments (where applicable)
- Updates policies in response to emerging threats
- Ensures lessons learned from incidents are embedded into practice

Security compliance is reviewed as part of:

- Internal audit cycles
- Safeguarding reviews
- Ofsted/ISI inspection readiness checks

9. Personal Data Breaches

Hopebright School treats all personal data breaches as **serious governance and safeguarding incidents**, with potential regulatory, legal, and reputational consequences.

A data breach is defined under UK GDPR as a **breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data**.

Types of Breach

A personal data breach includes (but is not limited to):

- **Loss or theft of data or devices**
    - e.g. laptops, USB drives, paper files, mobile devices
- **Accidental disclosure**
    - e.g. emailing data to incorrect recipients
    - printing or sharing information without authorisation
- **Cybersecurity incidents**
    - phishing attacks
    - ransomware or malware infections
    - unauthorised system access
    - compromised user accounts or credentials
- **Internal misuse of data**
    - accessing records without legitimate purpose
    - unauthorised sharing of pupil/staff data

All suspected breaches must be treated as real until confirmed otherwise.

Immediate Reporting Requirements

All staff must:

- Report suspected or actual breaches **immediately upon discovery**
- Notify the **Data Protection Officer (DPO)** without delay
- Escalate urgent safeguarding-related breaches to the **Designated Safeguarding Lead (DSL)** where applicable

Staff must not:

- Attempt to investigate independently
- Delay reporting while gathering full details
- Delete or alter affected records

Internal Incident Management

Upon notification, the School will:

- Record the incident in the **central Data Breach Register**
- Assign a unique incident reference number
- Log:

- Date/time of incident and discovery
- Nature of breach
- Data categories affected
- Individuals involved
- Immediate containment actions

The DPO will lead coordination with:

- Senior Leadership Team (SLT)
- IT/cyber security provider (where applicable)
- DSL (if safeguarding data is involved)

ICO Reporting Obligations

Where a breach is likely to result in a **risk to the rights and freedoms of individuals**, the School will:

- Notify the **Information Commissioner's Office (ICO) within 72 hours of becoming aware**
- Provide initial details even if full investigation is ongoing
- Submit follow-up reports as required

If the breach is unlikely to result in risk, it will be recorded internally but not reported to the ICO.

Communication with Affected Individuals

Where required, individuals will be informed without undue delay and provided with:

- A clear description of the breach
- Categories of data involved
- Likely consequences
- Measures taken to mitigate risk
- Advice on protective actions they should take

Communication will be:

- Clear, transparent, and age/role appropriate
- Approved by the DPO and SLT

Post-Incident Review and Learning

Following containment, the School will conduct a structured review to ensure continuous improvement and regulatory compliance.

This includes:

Root Cause Analysis

- How the breach occurred
- Whether procedural failure, human error, or technical weakness was involved
- Whether existing controls were sufficient

Corrective Actions

- Immediate containment effectiveness
- Policy or procedural updates required
- System configuration changes

Staff Response and Training

- Targeted retraining where human error is identified
- Reinforcement of data handling expectations
- Cyber awareness refresher training where required

System and Security Improvements

- Strengthening access controls
- Enhancing encryption or authentication
- Updating firewall, monitoring, or alert systems

All findings are documented and retained for **Ofsted/ISI inspection evidence and ICO audit readiness**.

10. Data Retention

Hopebright School retains personal data only for as long as necessary to fulfil its purpose, in line with statutory obligations and safeguarding best practice.

Retention is governed by a structured **Data Retention Schedule (Appendix 3)** and is regularly reviewed to ensure compliance with evolving legal and regulatory expectations.

Compliance Framework

Retention practices align with:

- **UK GDPR storage limitation principle**
- **ICO records management guidance**
- **Keeping Children Safe in Education (KCSIE 2025/26)**
- **Independent Schools Inspectorate (ISI) record-keeping expectations**
- Ofsted expectations for robust governance and safeguarding evidence trails

Core Retention Principles

The School ensures that all personal data is:

- **Necessary and proportionate** for its intended purpose
- **Regularly reviewed** to confirm continued relevance
- **Securely stored or archived** in approved systems only
- **Protected from unauthorised access throughout its lifecycle**
- **Deleted or anonymised securely when no longer required**

Secure Archiving and Disposal

Where data is no longer actively required but must be retained:

- It is securely archived in restricted-access systems
- Access is limited to authorised personnel only
- Audit trails are maintained

Where retention periods expire:

- Data is permanently deleted using secure deletion methods, or
- Anonymised where long-term statistical or reporting use is required

Deletion processes must ensure:

- Irrecoverability of data
- Removal from backups where feasible within system constraints

Review and Monitoring

The School undertakes periodic retention reviews to ensure:

- Compliance with updated legislation

- Removal of unnecessary or excessive data
- Alignment with safeguarding and operational needs

Retention compliance is subject to internal audit and may be reviewed during Ofsted or ISI inspections.

11. Data Accuracy

Hopebright School is committed to ensuring that all personal data held is accurate, complete, and kept up to date, in accordance with the UK GDPR principle of accuracy.

Accurate data is essential for safeguarding, operational effectiveness, and regulatory compliance.

Accuracy Assurance Measures

The School maintains data accuracy through:

- **Regular validation checks** across core systems (e.g. MIS, safeguarding databases)
- **Routine data cleansing processes** to remove duplication or outdated information
- **Structured parent/carer engagement** to ensure updates are reported promptly
- **Staff responsibility for real-time updates** following interaction with pupils or families
- **System audit trails** to track changes and corrections

Responsibilities for Data Accuracy

Parents and Carers

- Must notify the School promptly of changes to:
    - Contact details
    - Medical information
    - Emergency contacts
    - Legal custody arrangements (where applicable)

Staff

- Must ensure all records they create or update are:
    - Accurate at point of entry
    - Completed using approved systems only
    - Corrected immediately if errors are identified

School Systems and Administration

- Conduct periodic reconciliation of records across systems
- Identify inconsistencies between departments (e.g. admissions, safeguarding, attendance)

Importance of Accurate Data

Accurate data is critical for:

- **Safeguarding effectiveness**
    - Ensures correct emergency contacts and risk profiles are available
- **Ofsted inspection readiness**

    - Supports evidence-based evaluation of leadership and pupil outcomes
- **ISI compliance expectations**
    - Demonstrates robust governance and pupil oversight
- **Funding, census, and statutory reporting accuracy**
    - Ensures correct reporting to government bodies and examination boards

Correction of Errors

Where inaccuracies are identified:

- Corrections must be made **without undue delay**
- Where data has been shared externally, relevant third parties must be notified if necessary
- A record of correction may be retained where audit trail evidence is required

12. Information Requests

Hopebright School ensures all information requests are handled lawfully, consistently, and in line with statutory timescales and safeguarding obligations.

The School maintains a clear distinction between **educational records**, **Subject Access Requests (SARs)**, and **third-party disclosures**, ensuring transparency and accountability in all cases.

Educational Records

Educational records are provided in accordance with applicable education legislation and internal safeguarding controls.

- Requests will be responded to within **15 school working days**, where applicable under education regulations.
- Records may include:
    - Academic attainment and progress data
    - Behaviour and pastoral records
    - Attendance information
    - SEN support documentation (where applicable and appropriate for disclosure)

Where disclosure may present a safeguarding risk (e.g. third-party information, safeguarding notes, or confidential staff commentary), information may be:

- Redacted where lawful
- Withheld where disclosure would be likely to cause harm or breach third-party rights

All disclosures are subject to approval by the Data Protection Officer (DPO) or delegated senior leader.

Subject Access Requests (SARs)

Where requests fall under UK GDPR SAR provisions:

- Response timeframe is **1 calendar month**
- Extensions may apply for complex or multiple requests (up to 2 additional months, with justification)
- Identity verification is mandatory before disclosure
- Data will be provided in a secure format only

The School reserves the right to refuse or charge for:

- Manifestly unfounded requests
- Excessive or repetitive requests

Third-Party Sharing

Personal data is only shared where at least one of the following conditions applies:

- A **clear legal obligation** exists
- There is a **safeguarding requirement** under *Keeping Children Safe in Education (KCSIE 2025/26)*
- **Explicit informed consent** has been obtained (where appropriate and lawful)

All disclosures must follow the principle of **data minimisation**, ensuring only necessary information is shared.

Approved disclosure recipients include:

- **Exam boards and awarding organisations**
    - For registration, assessment, and certification purposes
- **Local authority safeguarding teams**
    - Where there is a child protection concern or statutory duty to refer/share information
- **Health services and medical professionals**
    - Where required to support pupil wellbeing, SEN provision, or emergency response
- **Regulatory bodies (e.g. Ofsted and ISI)**
    - Where lawful inspection or statutory reporting obligations apply
- **Law enforcement agencies**
    - Where required under legal request or serious safeguarding concern

All disclosures are:

- Logged in the School's information-sharing register
- Approved at appropriate senior level where sensitive data is involved
- Subject to proportionality and necessity checks

Information Security in Requests Handling

All staff handling information requests must:

- Use secure systems only
- Avoid sending personal data via unsecured email channels
- Verify identity before releasing any information
- Escalate uncertain or complex requests to the DPO

Failure to follow these procedures may result in disciplinary action and is treated as a potential data breach.

13. CCTV, Photography & Digital Media

Hopebright School operates CCTV and digital media practices in line with **ICO surveillance guidance, UK GDPR principles, safeguarding requirements, and inspection expectations for transparency and pupil protection**.

CCTV Systems

CCTV is used solely for:

- Safeguarding pupils, staff, and visitors
- Preventing and investigating crime
- Supporting site security and incident review

The School ensures:

- **Clear and visible signage** is displayed at all monitored locations
- CCTV usage is **proportionate and limited to stated purposes**
- Access is restricted to authorised personnel only (e.g. SLT, DPO, safeguarding lead)
- Footage is stored securely with access logging enabled
- Systems are protected against unauthorised access or cyber intrusion

Retention of CCTV

- Standard retention is **up to 30 days**
- Extended retention applies only where:
    - An incident is under investigation
    - Footage is required by law enforcement or safeguarding authorities
- All retained footage is securely archived and access-controlled

Photography and Video Recording

The School recognises photography and video as both a learning tool and a communication method but ensures strict consent and safeguarding controls are in place.

Photography/video may be used for:

- Educational activities and classroom learning
- Internal displays and school environment enrichment
- School communications and approved promotional materials

Consent Requirements

- **Explicit written consent must be obtained** from parents/carers (or pupils where appropriate by age/competence)
- Separate consent is required for:
    - Internal educational use
    - External marketing/publicity use
    - Website and social media publication

Consent is:

- Freely given, specific, informed, and revocable
- Reviewed periodically
- Recorded and stored securely within the School's MIS or consent management system

Withdrawal of Consent

Where consent is withdrawn:

- Future use of images/video will cease immediately
- Existing materials will be removed **where reasonably practicable**
- Materials already in printed circulation may not always be fully retractable but will not be reused

The School ensures withdrawal requests are actioned without delay.

Digital Media and AI Use

To meet 2026 digital governance expectations:

- AI-generated imagery, synthetic media, or automated content tools **must not use pupil personal data** unless:
    - A **Data Protection Impact Assessment (DPIA)** has been completed
    - Explicit authorisation has been granted by the DPO/SLT
- Staff must not upload identifiable pupil images to external AI tools or unapproved platforms

- Any new digital media tool or platform must undergo:
    - GDPR compliance review
    - Safeguarding risk assessment
    - Data processor due diligence

14. Staff Training

Hopebright School ensures all staff are appropriately trained to handle personal data securely and in line with evolving legal, safeguarding, and cyber security expectations.

Training is a key component of demonstrating compliance for **Ofsted and ISI inspections**, particularly in relation to leadership effectiveness, safeguarding culture, and operational risk management.

Mandatory Training Programme

All staff must complete:

Induction Training

- GDPR principles and lawful processing
- Data handling expectations
- Confidentiality and professional conduct
- Safeguarding-linked data awareness

Annual GDPR Refresher Training

- Updates to UK GDPR / DPA guidance
- Case studies of real-world breaches
- Role-specific responsibilities
- Changes in School policy or systems

Cyber Security Awareness Training

- Phishing and social engineering awareness
- Password security and MFA usage
- Safe use of email and cloud platforms
- Incident reporting procedures

Safeguarding & Data Handling Integration Training

- Safe handling of child protection information
- Information sharing thresholds under KCSIE
- Escalation pathways for concerns involving data

Role-Specific Training

Additional targeted training is provided for:

- Senior Leadership Team (data governance and breach decision-making)
- Designated Safeguarding Lead (DSL)
- Administration and admissions staff (data accuracy and SAR handling)
- IT/system administrators (cyber resilience and access control)

Monitoring & Compliance

- Training completion is tracked centrally
- Non-compliance is escalated to SLT
- Refresher training is mandated following:

- Data breaches
- Policy updates
- System changes
- Regulatory updates

Training records are retained as part of **Ofsted/ISI inspection evidence files**.

Appendix 1 – Data Breach Procedure

1. Purpose

This procedure sets out how Hopebright School identifies, reports, records, escalates, and responds to personal data breaches in compliance with **UK GDPR (Articles 33 and 34)**, the **Data Protection Act 2018**, and current **cyber resilience expectations for education settings (2026)**, including Ofsted and ISI governance standards.

A personal data breach includes any:

- Loss or theft of data or devices
- Unauthorised access to systems or records
- Accidental or unlawful disclosure of personal data
- Cybersecurity incidents (e.g. phishing, ransomware, malware infection, account compromise)

2. Immediate Action on Discovery of a Breach

Any staff member who suspects or identifies a breach must:

1. **Contain the incident immediately (where safe to do so)**
    - Disconnect affected device from network (if instructed or appropriate)
    - Stop further disclosure (e.g. recall emails if possible)
    - Secure physical documents
2. **Preserve evidence**
    - Do not delete files, emails, logs, or system alerts
    - Do not attempt independent investigation beyond containment
3. **Report immediately to the Data Protection Officer (DPO)**
    - Reporting must be **immediate and without delay**, regardless of certainty

3. Reporting Channels

All breaches must be reported to:

Data Protection Officer (DPO)

Email:

Out-of-hours emergency contact:

Reports must include:

- Date and time of discovery
- Description of incident
- Type of data involved
- Systems/devices affected
- Number of individuals impacted (if known)
- Immediate actions taken

4. DPO Assessment and Triage

The DPO will:

- Log the incident in the **Data Breach Register (centralised incident system)**
- Assess:

    - Severity (low / medium / high / critical)
    - Type of data involved (including special category data)
    - Likelihood and severity of risk to individuals
- Decide containment and mitigation actions
- Escalate to senior leadership if required

5. Escalation Levels

Level 1 – Low Risk

- No or minimal personal data exposure
- Internal logging only
- No ICO notification required

Level 2 – Moderate Risk

- Limited personal data exposure
- Containment required
- Possible ICO notification depending on risk

Level 3 – High Risk

- Sensitive or large-scale data exposure
- Mandatory escalation to SLT and safeguarding lead (if relevant)
- ICO notification considered or required

Level 4 – Critical / Major Cyber Incident

- Ransomware, system compromise, or large-scale breach
- Immediate escalation to:
    - Senior Leadership Team (SLT)
    - External IT/cyber security provider
    - ICO (within 72 hours)
- Potential notification to affected individuals without delay

6. ICO Notification Requirement

Where risk to individuals is likely:

- ICO must be notified **within 72 hours of awareness**
- If full details are not available, initial notification must still be made with updates provided later

---

7. Communication with Affected Individuals

Where required:

- Individuals will be informed without undue delay
- Communication will include:
    - Nature of breach
    - Data involved
    - Potential consequences

    - Steps taken by the School
    - Advice for affected individuals

8. Post-Incident Review

After containment:

- Root cause analysis conducted
- System vulnerabilities identified
- Preventative actions implemented
- Staff retraining completed if required
- Cyber security controls reviewed and strengthened

9. Record Keeping (Mandatory)

All breaches must be recorded in the **Data Breach Register**, including:

- Timeline of events
- Decisions made and rationale
- Risk assessment outcome
- ICO notification details (if applicable)
- Lessons learned and corrective actions

Records must be retained for audit purposes (Ofsted/ISI compliance evidence).

Appendix 2 – Data Breach Report Form (Confidential)

This form must be completed immediately upon discovery of a suspected or actual data breach.

1. Incident Details

- Date of breach:
- Time breach identified:
- Location / system affected:
- Reported by:
- Job role:

2. Description of Incident

Provide a clear summary of what happened:

- Nature of breach (loss / theft / disclosure / cyber attack / other):
- How the breach occurred:
- Was the breach ongoing at time of report? (Yes/No):

3. Data Involved

- Type of data (tick all that apply):
    - ☐ Personal data
    - ☐ Special category data
    - ☐ Safeguarding data
    - ☐ Financial data
    - ☐ Staff data
    - ☐ Pupil data
    - ☐ Other (specify):
- Approximate number of individuals affected:
- Categories of individuals affected:
    - ☐ Pupils
    - ☐ Staff
    - ☐ Parents/carers
    - ☐ External stakeholders

4. Containment Actions Taken

- Immediate actions taken:
- Has access been restricted or systems isolated? (Yes/No)
- Has data been recovered or secured? (Yes/No/Partial)

5. Risk Assessment (DPO Use Only)

- Risk level assigned:
    - ☐ Low
    - ☐ Medium

    - ☐ High
    - ☐ Critical
- Rationale:

6. ICO Notification

- ICO notified? (Yes/No/Pending)
- Date/time notified:
- Reference number (if provided):

7. Communication

- Have individuals been informed? (Yes/No/Pending)
- Date of communication:
- Method used (email/letter/other):

8. Actions and Outcomes

- Immediate corrective actions:
- Long-term preventative measures:
- System/process changes required:

9. DPO Sign-Off

- Name:
- Signature:
- Date:

10. Storage Instructions

This form must be:

- Stored securely within the **School's Incident Management System**
- Access restricted to:
    - DPO
    - Senior Leadership Team
    - Safeguarding Lead (if relevant)
- Not stored on personal devices or unsecured email accounts

Appendix 3 – Data Retention Schedule

Pupil Records

- SEN files: up to 35 years from DOB
- Pupil records: 25 years from DOB
- Attendance: 6 years
- Exam results: 7 years after leaving

Safeguarding (Enhanced)

- Child protection records: **indefinite retention (best practice safeguarding standard)**
- Allegations against staff: until retirement age + safeguarding review period
- DBS records: not retained beyond statutory limits

Staff Records

- Employment records: 7 years post-employment
- Payroll: 7 years
- Recruitment (unsuccessful): 6 months
- Right to work checks: 2 years post-employment

Financial Records

- Accounts/tax: minimum 6 years
- Contracts: 7–13 years depending on type

CCTV

- Typically 30 days unless required for investigation