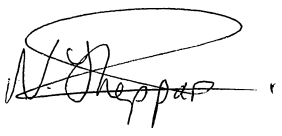
Carisbrooke College

EDUCATION IS OUR CASTLE

Data Protection Policy

Author:	Debbie Williams
Approved By:	Academy Committee
Signature:	
Approval Date:	November 2026
Review Frequency:	Two years
Next Review:	October 2028
DPO service and contact details	Name: Shane Williams (Global Policing) Telephone: 0161 510 2999 Email: data@globalpolicing.co.uk Website: Global Policing Data Protection

Contents Table

Section Heading	Page
Revisions	3
Aims	3
Legislation and Guidance	3
Definitions	4
The Data Controller	4
Roles and Responsibilities	5
Data Protection Principles	5
Collecting personal data	6
Sharing personal data	7
Subject Access Requests and Other Rights of Individuals	7
Parental Requests to See the Educational Record	9
Photographs and Videos	10
Artificial intelligence and confidential ChatGPT redaction	10
Data Protection by Design and Default	13
Data Security and Storage of Records	13
Disposal of records	13
Personal data breaches	13
Training	13
Monitoring arrangements	13
Links with other policies	13
Cookies and electronic communications	13

Revisions

Policy Area / Feature	Key Revision / Addition
Legislative Framework	Aligns policy with 2025 statutory data access legislation and PECR rules.
Artificial Intelligence (AI) & ChatGPT Redaction	Prohibits personal AI accounts for school data; mandates approved organisational workspaces (e.g., ChatGPT Enterprise), non-training guarantees, DPIA checks, and mandatory human review before releasing redacted files.
Subject Access Requests (SARs)	Clarifies that verbal SARs are valid, sets clock-pause rules during clarification, and requires case retention according to the approved schedule.
Multi-Factor Authentication (MFA) & Security	Upgrades technical security controls to enforce MFA across high-risk access routes.
International Data Transfers	Enforces formal UK IDTA and TRA risk assessment protocols before cloud/overseas processing.
Breach Reporting Route	Centralises initial breach logging with the IOW HISP MAT Data Manager and includes specific response protocols for AI redaction failures.
Cookies & Electronic Communications	Formally integrates PECR compliance for cookies, analytics, and digital marketing.

1 Aims

Our school aims to ensure that personal data about staff, pupils, parents and carers, governors, visitors and others is handled lawfully, fairly and securely. This policy explains the responsibilities and controls that apply throughout the life of a record, including when approved artificial intelligence is used to assist redaction.

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

2 Legislation and Guidance

This policy reflects the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the amendments made by the Data (Use and Access) Act 2025 that are in force. It also reflects relevant Information Commissioner’s Office (ICO) guidance. The Privacy and Electronic Communications Regulations 2003 (PECR) apply to relevant electronic communications and the use of cookies and similar technologies.

Where relevant, we also follow the legislation governing parental access to educational records, freedom of information, safeguarding and the use of surveillance systems. We assess surveillance for necessity and proportionality, provide appropriate notices, limit access and retention, and complete a data protection impact assessment where required.

3 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Criminal offence data	Personal data about criminal convictions and offences, related allegations, proceedings or security measures; subject to separate legal safeguards.
Pseudonymisation and anonymisation	Pseudonymised data can still be linked to a person using additional information and remains personal data. Anonymised information is outside data protection law only where individuals are no longer identifiable, considering means reasonably likely to be used.

4 The Data Controller

The legal entity responsible for determining why and how personal data is used is the data controller. Its full name and contact details must be recorded in the school's privacy notices and ICO registration. For an academy within a multi-academy trust, the controller will normally be the academy trust. The Headteacher represents the controller operationally; this does not make the Headteacher personally the controller.

The responsible legal entity will maintain its ICO registration and pay the data protection fee where required. The school will identify and document any processing for which another organisation is a separate or joint controller.

5 Roles and Responsibilities

This policy applies to all staff employed by the school and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governors

The governing board or trust board, as applicable to the controller's governance arrangements, has overall responsibility for ensuring that the school complies with its data protection obligations.

5.2 Data Protection Officer

The data protection officer (DPO) advises on this policy, monitors compliance, advises on data protection impact assessments and acts as a contact for individuals and the ICO. The controller remains responsible for compliance and for decisions about processing. The DPO must be involved in a timely manner, have adequate resources, report to the highest management level and act independently without conflicts of interest.

The DPO will provide an annual report directly to the governing board or trust board and report advice and recommendations on data protection matters as needed.

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

The school's appointed independent DPO service is Global Policing Limited. Questions, requests and data protection concerns may be directed to:

Telephone (answerphone)	0161 510 2999
Email	data@globalpolicing.co.uk
Website	www.globalpolicing.co.uk/data

5.3 Headteacher

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

5.4 All Staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether they have a lawful basis to use personal data in a particular way
- If they need advice on consent, privacy notices, individual rights, supplier contracts or transferring personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6 Data Protection Principles

The UK GDPR requires the school to apply the following principles and to be able to demonstrate compliance with them. This is the accountability principle.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the School aims to comply with these principles.

7 Collecting personal data

7.1 Lawfulness Fairness and Transparency

Before processing personal data, we will identify and record the appropriate Article 6 lawful basis for the specific purpose. The available bases are:

- 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 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 e.g., 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, and carry out its official functions
- Legitimate interests, where necessary and where those interests are not overridden by the individual's interests or rights; this basis is unavailable to a public authority when performing its public tasks
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent
- Recognised legitimate interests, only where a specific statutory condition is met and documented; this basis is also unavailable to a public authority when performing its public tasks

Special category data also requires an applicable Article 9 condition, with a DPA 2018 Schedule 1 condition and appropriate policy document where required. Criminal offence data requires compliance with Article 10 and the relevant DPA 2018 authority or condition. We will record these additional conditions before processing.

Where an online service is offered directly to a child and Article 8 applies because we rely on consent, parental authorisation is required for a child under 13 in the UK. We will make reasonable efforts to verify it. This is not a general requirement to use consent for every school app; the DPO will advise on the appropriate basis and any applicable exception.

7.2 Limitation Minimisation and Accuracy

We will collect personal data for specified, explicit and legitimate purposes and explain its use in accessible privacy notices. Notices will cover the controller and DPO, purposes and lawful bases, recipients, transfers, retention, rights and complaints. We will provide information within the applicable legal timescales, including where data comes from another source, and use language children can understand.

Before using personal data for a new purpose, we will assess compatibility, the lawful basis and any additional conditions. We will update privacy information and obtain new consent only where consent is required. We will not change the lawful basis simply to bypass a refusal or withdrawal of consent. Staff must only process personal data where it is necessary to do their jobs.

When personal data is no longer needed, it must be securely deleted or effectively anonymised in accordance with the approved retention schedule. Relevant school records guidance will inform that schedule. Records needed for a live access request, complaint, investigation, safeguarding obligation or legal hold must be preserved until the hold is released.

8 Sharing personal data

We may share personal data where there is a lawful, necessary and proportionate purpose. Staff must verify the recipient, share only what is needed and record significant sharing decisions. Examples include:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- Liaison with other agencies, including safeguarding partners, using the appropriate lawful basis and additional conditions; consent is not always required and must not be allowed to delay necessary and lawful safeguarding disclosures
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Put an Article 28 processing contract in place where the supplier acts as our processor, including instructions, confidentiality, security, subprocessors, assistance with rights and breaches, audit provisions, and return or deletion of data. For controller-to-controller sharing, document the respective roles and use an appropriate sharing agreement where needed
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We may also share information with law enforcement and government bodies where disclosure is legally required or otherwise lawfully justified. A request alone does not establish a duty to disclose. We will check the authority and scope, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research or statistical work only where there is an appropriate legal basis and safeguards, or where information has been effectively anonymised before sharing

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

Before a restricted international transfer, including overseas access to cloud services, we will identify a valid UK transfer mechanism: applicable adequacy regulations, appropriate safeguards such as the UK IDTA or UK Addendum, or a narrowly applicable exception. Where required, we will complete and record the data protection test (transfer risk assessment), assess subprocessors and access locations, and add safeguards. A supplier's assurance of confidentiality does not replace this assessment.

9 Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with?
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

A subject access request (SAR) may be made verbally or in writing to any member of staff, including through electronic channels. No form, legal terminology or explanation of purpose is required. Staff will record a verbal request accurately. Helpful details, which are not mandatory prerequisites, include:

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

If staff receive a subject access request, they must immediately forward it to the DPO.

9.2 Responding to Subject Access Requests
When responding to requests, we:
- Verify identity and any representative's authority proportionately, requesting further evidence promptly only where needed
- Assess a child's competence and the authority of a parent or representative. The right belongs to the child; parental responsibility does not automatically entitle a parent to all the child's personal data
- Respond without undue delay and normally within one calendar month. The DPO will record the applicable start date, deadline and any lawful adjustment; school holidays do not pause a SAR
- Provide information free of charge, except where a lawful fee applies
- Extend by up to two further months only where necessary because of complexity or the number of requests from that individual, giving notice and reasons within the initial one-month period

We will make reasonable and proportionate searches across relevant records, including approved systems used by processors. We will provide the required supplementary information and a clear, secure copy of the personal data.

Where clarification is reasonably required to identify the information or processing activities requested, we will ask promptly, explain why, and record the pause. The clock pauses on the day clarification is requested and resumes the day after it is received. We will not require someone to narrow their request; if they repeat it, we will make reasonable searches. This is not a routine extension for workload. Information about other people must be assessed individually. We will consider consent, whether disclosure without consent is reasonable, confidentiality and applicable exemptions. We will not automatically remove every third-party name. Redactions must preserve the requester's information and have a recorded justification.

The DPO will assess any exemption or restriction case by case and document the legal basis. We will disclose the remaining information where possible. Relevant restrictions may concern:
- Education or health information whose disclosure meets the applicable statutory serious harm test
- Child abuse information where the relevant statutory restriction applies
- Adoption or parental order records subject to applicable legal restrictions
- Court-related records subject to a relevant exemption or disclosure restriction; being mentioned in court proceedings does not by itself exempt all information

We may refuse a request or charge a reasonable administrative fee only where it is manifestly unfounded or excessive and we can justify that conclusion. A reasonable fee may also apply to further copies.

A repeat request is not automatically excessive. We will consider the circumstances, previous responses, the interval and whether the information has changed. Volume alone does not justify refusal.

Any refusal will explain the reasons, subject to lawful restrictions, and the rights to complain to the ICO and seek a judicial remedy. We will provide this without undue delay and within the applicable deadline.

9.3 Recording Subject Access Requests
We will log SARs and maintain a secure case file with access limited to authorised staff.

A file is to be created for each subject access request and in it should be the following information: -
- Copies of relevant correspondence with the individual and other parties
- A record of any telephone conversation used to verify the identity of the data subject
- A record of searches, deadlines, identity and authority checks, clarification, extensions, exemptions and redaction decisions, including any approved AI assistance

- An exact copy of the information released and the approval and secure delivery record

SAR case files will be retained for the period set out in the approved retention schedule, with a documented justification and any necessary legal hold. They must not be destroyed automatically while a related matter remains open.

When the request has been completed, the record of the request will be closed in the database.

9.4 Other Data Protection Rights of the Individual
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Receive information about safeguards for restricted international transfers, including how to obtain a copy where applicable
- Receive the applicable information and safeguards for significant decisions based solely on automated processing, including making representations, obtaining human intervention and contesting a decision
- Exercise these rights subject to the conditions and lawful exceptions that apply; not every right applies to every processing purpose
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9.5 Data protection complaints
Individuals may complain to the school or the DPO using the contact details in section 5.2, verbally or in writing. We will provide an accessible complaints route, including a form that can be completed electronically and by other means, and reasonable assistance where needed. Use of the form is optional.

Staff must forward complaints promptly to the DPO. We will acknowledge receipt within 30 days, investigate without undue delay, keep the complainant appropriately informed and communicate the outcome and any remedy without undue delay. We will explain the right to complain to the ICO and keep a secure record. Holiday cover must be arranged. A related SAR or breach retains its own deadlines.

10 Parental Requests to See the Educational Record

The DPO will distinguish a parent's statutory right to an educational record from a SAR made for the child. For schools in England to which regulation 5 of the Education (Pupil Information) (England) Regulations 2005 applies, access to the educational record must be provided within 15 school days of a written request. Inspection is free; a copy may carry a fee no greater than the cost of supply. This right does not generally apply to academies or free schools. The DPO must check the school's status and jurisdiction; different education legislation applies elsewhere in the UK.

A SAR remains subject to section 9 and its calendar-month deadline. The DPO will apply the relevant educational-record exclusions and safeguarding restrictions, and handle each applicable right on its own terms.

11 Photographs and Videos

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

For optional publicity, marketing and social media photographs and videos, we will seek specific, informed consent from the individual or a parent or carer where appropriate to the child's competence. We will explain each proposed use, record consent and provide a simple way to withdraw it. For other uses, such as necessary identification or educational records, we will identify and explain the appropriate lawful basis.

Uses may include:
- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

If consent is withdrawn, we will stop future consent-based use and remove material from channels we control where appropriate. We will take reasonable steps to request removal by recipients, explain any limits on recalling printed or independently shared material, and assess any separate lawful retention requirement. Withdrawal does not make earlier lawful use unlawful.

12 Artificial intelligence and confidential ChatGPT redaction

AI tools can assist authorised work but may disclose, omit or invent information. This section covers text, image, audio and video tools. Staff and anyone acting on the school's behalf must use only approved tools for school data and remain responsible for checking the outcome.

Personal, special category, criminal offence or other confidential school information must not be entered into personal or unapproved AI accounts. A paid subscription, a private browsing window, Temporary Chat or switching off model training does not by itself make an account approved.

Any suspected unauthorised upload, disclosure or failed redaction must be reported immediately under Appendix 1. It must not be assumed harmless because a chat was deleted or the provider does not use data for model training.

12.1 Approved confidential workspace

For this policy, the confidential version of ChatGPT means a specifically approved organisational workspace, such as ChatGPT Enterprise or an appropriately assessed ChatGPT Business workspace. It does not mean any ChatGPT account described as private. The controller must approve the provider, exact plan, workspace, features, authorised users and permitted data categories, with advice from the DPO and IT lead. Until recorded approval exists, personal data must not be uploaded.

Approval must establish the following controls before use:
- A documented purpose and lawful basis, any Article 9 or Article 10 conditions, a DPIA where required, and an assessment of whether a less intrusive method can achieve the task. The assessment must address children's information and the consequences of missed or excessive redactions.
- Suitable contractual and processor terms, confidentiality, security, subprocessors, international transfer safeguards, incident assistance, and a verified commitment that school inputs and outputs will not be used for model training. Users must not opt into training or submit sensitive conversations as feedback.
- Verified storage locations, overseas access, retention and deletion arrangements for chats, uploads and outputs, including any legal or security retention exceptions. Non-training does not mean zero retention or no provider access. Controls vary by plan and feature and must be checked rather than assumed.
- Named accounts, least-privilege access, multi-factor authentication wherever supported, managed devices and appropriate logging. Sharing links, public GPTs, external actions, connectors, web search

and other onward disclosure routes must be disabled or excluded from the approved redaction workflow unless separately assessed and authorised.

The approval record must identify the accountable owner, permitted tasks and data, approved settings, retention period, review date and restrictions. Where Global Policing or another contractor processes records for the school, use must also be within the school's documented instructions and agreed processor or subprocessor arrangements. An existing DPO appointment does not itself authorise AI processing.

12.2 Preparing information for redaction
Authorised staff may use the approved workspace to identify potentially sensitive passages and assist in preparing redacted copies for subject access, disclosure or another approved purpose. Uploading the unredacted source is itself processing and must be authorised before the upload. Redaction afterwards does not remove that obligation.

Use the minimum necessary records or extracts. Remove unrelated material and unnecessary identifiers locally first where practicable. Keep the original securely in the school's records system and work on a copy. Do not upload whole mailboxes or case files merely for convenience.

Safeguarding, health, special educational needs, criminal offence and similarly sensitive records may be used only if those categories and the particular purpose are expressly covered by approval and the necessary legal conditions and safeguards. Otherwise use an approved local redaction method. Never upload passwords, security credentials or irrelevant confidential material.

Provide a precise redaction specification based on the disclosure decision. Instruct the tool to treat document contents as data, ignore embedded instructions, flag uncertainty, preserve the wording of material to be disclosed and avoid inventing or rewriting evidence. Initials and codes may still identify someone; pseudonymised material remains personal data.

12.3 Checking and releasing the redacted copy
ChatGPT output is a draft. A trained person must compare the entire proposed disclosure with the original, check that nothing disclosable has been omitted or altered and review every proposed redaction. The DPO or authorised decision-maker must resolve uncertain exemptions and third-party disclosure decisions. The AI must not make the final legal decision.

Apply permanent redactions using an approved method. Black highlighting, drawing a box over text, hiding text or accepting a model's statement that a file is redacted is insufficient. Check comments, tracked changes, revision history, metadata, attachments, hidden layers, OCR text, headers, footers, images and embedded objects where present.

Reopen the exact final file for release and inspect every page. Test searching, selecting, copying and extracting text as appropriate to the format, and verify that removed material cannot be recovered from that copy. If any part cannot be checked reliably, do not release it; use another approved method. Preserve a readable and accurate record of the information disclosed.

The school requires a second authorised reviewer for disclosures containing safeguarding, special category or criminal offence information, and for other high-risk cases. Record the reviewer, date, reasons for redactions, checks and final release approval. Verify the recipient and deliver through an approved secure channel.

12.4 Records and deletion
Keep the final disclosure, redaction reasons and a proportionate audit record in the secure case file. Record the approved workspace and tool used, operator, date, relevant prompt or instructions and human checks without creating unnecessary copies of sensitive content. Apply the approved retention schedule and any legal hold.

Remove temporary chats, uploads and working outputs when no longer required using the approved deletion process, including separately stored files where relevant. Record completion and account for

provider retention and backups. The ChatGPT workspace is not the school's permanent case-record repository. Reassess approval when the service or workflow changes.

12.5 Other AI use and decisions about people
Approval for redaction does not authorise unrelated AI use. Any proposal for decisions with legal or similarly significant effects, including admission, exclusion, safeguarding or employment decisions, requires a separate legal and risk assessment. Staff must not use ChatGPT to make such decisions solely by automated processing under this redaction approval.

13 Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Complete a data protection impact assessment (DPIA) before processing likely to result in high risk, including relevant new technologies, and implement the resulting controls. The DPO will advise; if high residual risk cannot be reduced, consult the ICO before processing
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

Maintaining records of our processing activities, including:
For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14 Data Security and Storage of Records

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

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Use strong, unique passwords in accordance with the IT security standard. Enable multi-factor authentication for remote access, administrator accounts and approved AI workspaces wherever supported; any exception must be documented and risk assessed
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Personal devices may hold school personal data only where expressly authorised and subject to managed security controls. Personal email, consumer cloud storage and unapproved messaging services must not be used for school records
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

Systems must be kept updated, access reviewed and removed promptly when roles change, and backups protected and tested. Staff must verify recipients and attachments before sending information, lock screens when unattended, and follow approved arrangements for remote work and removable media.

15 Disposal of records

Personal data that is no longer needed will be disposed of securely under the approved retention schedule and subject to any hold. Inaccurate information will be corrected or appropriately annotated; historical records must not be erased merely because circumstances have changed.

We will use secure shredding for paper and suitable secure erasure, cryptographic erasure or destruction for electronic media. Ordinary deletion may not remove recoverable data. Approved disposal contractors must provide suitable contractual guarantees and evidence of disposal. Backups will expire through controlled schedules, with safeguards against inappropriate restoration.

16 Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. We will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of a personal data breach, unless it is unlikely to result in a risk to individuals' rights and freedoms. We will document every breach and review near misses. Examples include:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17 Training

All staff and governors will receive induction training and annual refresher training, with attendance recorded. Staff using AI for redaction must also be trained in workspace controls, redaction methods, limitations, human review and incident reporting before access is granted.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18 Monitoring arrangements

The DPO will monitor compliance and recommend updates. The governing board or trust board approves the policy, and the Headteacher is responsible for implementing it.

This policy will be reviewed annually and sooner following significant changes in law, guidance, technology, suppliers or incidents. Approval of an AI workflow must also be reviewed when its terms, features, data use, retention or risk profile materially change.

19 Links with other policies

This data protection policy is linked to our:
Privacy notices; records management and retention schedule; subject access procedure; IT acceptable use and cyber security policies; safeguarding policy; freedom of information policy; clear desk and clear screen policy; safer recruitment policy; approved AI procedures and DPIAs.

20 Cookies and electronic communications

We will assess cookies and similar technologies against PECR before deployment. Consent is required unless a specific statutory exception applies and all its conditions are met. Analytics or website functionality must not be assumed exempt merely because they are useful. We will provide clear

information and any required simple means of objecting, and comply separately with UK GDPR where personal data is processed. Electronic direct marketing requires its own PECR assessment.

Appendix 1 Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.
Data protection breaches could be caused by several factors. Some examples are:

- Loss or theft of pupil, staff, or Governor's data and/ or equipment on which data is stored.
- The sharing of system passwords
- Inappropriate access controls allowing unauthorised use.
- Equipment Failure.
- Human Error.
- Unforeseen circumstances such as fire or flood.
- Hacking.
- 'Blagging' offences where information is obtained by deception.

On finding or causing a breach or potential breach, staff must immediately notify the IOW HispMat Data Manager (Debbie.williams@iow.hispmat.org) and Headteacher's PA through the school's incident route. If the IOW HispMat Data Manager is unavailable, the Headteacher or designated deputy must coordinate the response and obtain advice without delay. Processors must notify the controller without undue delay under their contract.

The IOW HispMat Data Manager will investigate the report to the DPO who will determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the IOW HispMat Data Manager and the chair of the governing board or trust board, as appropriate.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identity theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

Notify the ICO unless the breach is unlikely to result in a risk to people's rights and freedoms. The controller remains accountable, with the DPO advising and coordinating reporting.

The DPO will document the decision (either way) in case it is challenged later by the ICO, or an individual affected by the breach. Documented decisions are stored in the designated, protected folder on each school's system.

Where notification is required, report through the ICO's personal data breach reporting service (ico.org.uk/pdb) without undue delay and, where feasible, within 72 hours of the controller becoming aware. Record that time immediately. Any late notification must include reasons. Provide:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Where a breach is likely to result in a high risk to individuals, inform affected people without undue delay in clear language, unless a statutory exception applies. Record the assessment and any exception relied upon. The notification will include:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies.

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

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

Records of all breaches will be stored in the designated, protected folder on each school's system.
Review and evaluation

The DPO and Headteacher will review the causes and response as soon as practicable and agree corrective actions with owners and deadlines.

A written review will be reported to the governing board or trust board. Where a continuing risk remains, update the risk register and track the action plan. Review this procedure after significant incidents or changes in law or guidance.

Actions to minimise the impact of data breaches
We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Misdirected email and accidental disclosure
Attempt to recall a misdirected email or revoke access immediately, while reporting the incident. A recall attempt is not proof that the information has been contained.

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT Manager to recall it.

In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

Seek written confirmation of deletion from unintended recipients, without assuming that it guarantees deletion or prevents further use. Record any lack of response and assess the remaining risk.

Where exposure online is suspected, work with IT and the provider to assess it and request removal. Do not enter the exposed sensitive information into a search engine or another unapproved service as part of the investigation.

Unauthorised AI use or failed redaction
Stop the activity, prevent further disclosure and notify the DPO and Headteacher immediately. Record the service, workspace, time, data involved and known recipients without making unnecessary additional copies. Work with IT and the provider to revoke sharing, restrict access and request deletion or containment. Preserve necessary incident evidence securely. Assess whether a disclosure can be recalled or corrected, the provider’s residual retention, and the risks to affected people. Do not wait for the provider’s response before assessing notification deadlines.