Data Protection Policy

Version	Date	Summary of Changes
1.0	14/05/2018	Initial Version
1.1	12/11/2018	Page 2 – paragraph 5.2 DPO changed to i-West@bathnes.gov.uk Page 10, Paragraph 16, removed and inserted into Records Management Policy Page 11, Appendix 1 bullet point 2 wording amended from investigate to advise and manage Appendix 2 – Data Incident Reporting Form added
1.2	04/05/2021	Pages 5, 6, 8, 9 - References to EU GDPR changed to UK GDPR
	04/05/2021	Page 10 - Review Period changed from every 2 years to annually
	04/05/2021	Pages 14 and 15 - Appendix 3: Security Incident Management: Record of Work Removed
1.3	25/05/2023	Changes to legislation (UK GDPR)
1.4	19/11/2024	Additional information added on the lawful basis for processing special category data (page 6), accountability principles added (page 6), SARs can be

		made verbally (page 8), controls added re locking devices (page 11) and BYOD (page 11 & 12), updated breach procedure (page 12 and Appendix 1).
1.5	18/11/2025	Reference to the Data Use and Access Act (DUAA 19 June 2025), additional responsibilities re checking emails sent/received and the risks associated with both – plus other minor changes and comments.

Approved by Governors: 1 December 2025
Review Date: December 2026

Contents

Aims

Our school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Legislation.

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

This policy also acts as our appropriate policy document for the processing of special category personal data.

Legislation and guidance

This policy meets the requirements of the UK GDPR, the Data Use and Access Act 2025 (DUAA) and of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

The ICO's Guidance on CCTV can be found here.

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

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.

The data controller

Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO (Z6075094) and will renew this registration annually or as otherwise legally required.

Roles and responsibilities

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

Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

Full details of the DPO's responsibilities are set out in the Service Level Agreement between the school and the DPO.

Our DPO is from i-West, part of Bath & North East Somerset Council's trading arm (One West) and is contactable via the email address: i-West@bathnes.gov.uk.

Headteacher

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

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 or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the 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

Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- 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.

There is also an accountability principle, and this policy sets out how the school aims to comply with the principles above.

Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual 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 – the majority of our processing is done under this lawful basis.
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent** (for example for the use of student photographs for promotional purposes).

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in Article 9 of the UK GDPR, and conditions under Schedule 1 Part 2 of the Data Protection Act 2018 for processing under substantial public interest.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law – we do this primarily through our Privacy Notices (see link below).

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data, and we do this through our Privacy Notices which are available on our website here:

https://www.cotham.bristol.sch.uk/page/?title=Privacy+Notices&pid=241

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary, or inform you of the lawful basis (if not consent).

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Retention Schedule which is part of its Record Management Policy – this can be found using the link above.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this, or identify another lawful basis.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – 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
    - Establish a data sharing or processing agreement when applicable with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, 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 and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

Where we transfer personal data internationally we will do so in accordance with UK data protection law, and will ensure there are appropriate safeguards in place so that suitable protections are in place.

Subject access requests and other rights of individuals

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

Subject access requests do not have to be made in writing. However, for any SARs received verbally the school may follow up in writing with the requester (for example to clarify the scope of the request or to formally acknowledge the request). If staff receive a subject access request they must immediately forward it to the Compliance, Information and Governance Officer.
The link to the SAR form here.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the views of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide identification so the individual can be verified.
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- Will conduct a 'reasonable search' for the information within scope

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be manifestly unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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, individuals also have the right to:

- Withdraw their consent to processing at any time (where the processing is based on consent)
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the UK
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data that has been provided to us 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.

Parental requests to see the educational record

Parents, or those with parental responsibility, can request access to their child's educational record (which includes most information about a student).

The annual school report is the normal process by which educational records are disclosed, and for any further information on the student record this will be processed under our SAR procedures.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to CCTV and video surveillance | ICO.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded through signage, this policy, and our Privacy Notices.

Any enquiries about the CCTV system should be directed to Ed Carpenter, Deputy Director of Finance and Resources - IT and Facilities Lead.

Photographs and videos

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

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used. Examples where consent is not needed would be personal use (i.e. parent taking a photo of their child at a school show/event) or photo taken for ID purposes.

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

Consent can be refused or withdrawn at any time. If you change your mind at any time, you can let us know by emailing info@cotham.bristol.sch.uk, or by completing a new Photograph/Video Consent Form (available from school office, or on our website). If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with full names, to ensure they cannot be identified.

See our child protection and safeguarding policy and publications policy for more information on our use of photographs and videos.

Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing Data Protection Impact Assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and Privacy Notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; 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, any transfer outside of the UK and the safeguards for that, retention periods and how we are keeping the data secure

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.
- Devices are locked when left unattended (Windows Button ⏵ + L is a handy shortcut).
- Papers containing confidential personal data must not be left on display on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access, and must be suitably secured when left unattended.
- Where personal information needs to be taken off site, it will be encrypted, and for paper based records staff must ensure these are suitably protected in transit (e.g. not left on a seat, but held in a receptacle and in the boot) and at rest (e.g. stored out of sight when at home – for example in a work bag or where possible locked away).
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Staff to double check the accuracy of recipient's email address, any attachments and information within any email trail for correctness, and when emailing multiple recipients whether the email should be sent using BCC (when sending emails)
- Staff to not respond, click links, or open attachments (when receiving emails) from any sender where they are not expecting the email, and the email does not look and feel right – checks must be made to verify the requester (not via email, but by other trusted means such as a phone call or SMS taken from a genuine source).
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, students or governors who process school personal information on their personal devices (such as remote access, or accessing webmail) are:
    - Expected to follow the same security procedures as for school-owned equipment (see our Online Safety Policy)
    - Able to ensure:
        - the device is protected by a PIN or password
        - that passwords to any school applications or systems are not saved to browsers or operating systems
        - that applications and systems are properly logged out of after use
        - that devices are locked when left unattended
        - that such devices are not used for taking images/footage of students/students.
        - that school data is not saved locally to the device
        - that the latest updates are applied to the device

- 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).

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.

For any breaches where we consider there is a high risk to the rights and freedoms of the affected individuals, the school will ensure the breach is reported to the ICO usually within 72 hours, and to the affected data subjects as soon as practically possible. The school's DPO will advise on all data breaches.

Training

All staff and governors are provided with data protection training as part of their induction process.

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

Monitoring and review

- The DPO is responsible for monitoring and reviewing this policy.
- This policy will be reviewed annually. Approval has been delegated by the full governing board to the Finance, Premises & General Purposes Committee, with updates reported to the full governing board for information.
- Any incidents occurring during the school year will be evaluated and where necessary appropriate action will be taken to amend the policy accordingly.

Links with other policies

This data protection policy is linked to our:

- Freedom of Information Policy
- Child Protection and Safeguarding Policy
- Online Safety Policy

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the school Compliance, Information and Governance Officer, who will contact the DPO for further advice.
- The DPO will advise and manage the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Compliance, Information and Governance Officer will alert the headteacher and the chair of governors.
- The Compliance, Information and Governance Officer 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 advise the school on 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
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
      If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the School's own internal secure computer network as well as within the files of our contracted out provider i-West.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will advise the Compliance, Information and Governance Officer to promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - 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 on the school's own internal secure computer network as well as within the files of our contracted out provider i-West.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

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.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the Compliance, Information and Governance Officer as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the ICT department will be asked to recall it if this is technologically possible
- In any cases where the recall is unsuccessful, the relevant unauthorised individuals who received the email will be contacted, informed that the information was sent in error, and requested that those individuals delete the information and do not share, publish, save or replicate it in any way
- We will require a written response from all the individuals who received the data, confirming that they have complied with this request
- An internet search will be carried out to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Appendix 2: Data Incident Reporting Form

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation	*If there was any delay in reporting the incident, please explain why this was*
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why?	*Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes.*
2. Recovery of the data	
What have you done to contain the incident?	*eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects*
Please provide details of how you have recovered or attempted to recover the data, and when	*Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	
Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	
Have any of the affected individuals made a complaint about the incident?	
Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?	
Your name and contact details:	