



COLCHESTER COUNTY HIGH SCHOOL FOR GIRLS

A19 Data Protection Policy

COMMITTEES	HR and Wellbeing Committee & Curriculum & Student Matters Committee
CCHSG DATA PROTECTION LEAD	Lesley Pye Data & Administration Manager
CCHSG SENIOR INFORMATION RISK OFFICER (SIRO)	Kelly Sharp Assistant Principal
DATA PROTECTION OFFICER	Lauri Almond Information Governance Manager Contactable via Essex County Council, 03330 322970 (igs@essex.gov.uk)
REVIEW	Annually
POLICY REVIEWED	October 2025
REVIEW DUE	October 2026
APPROVED BY THE GOVERNING BODY	November 2025

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions	3
4. The Data Controller.....	4
5. Roles and responsibilities	4
6. Data Protection Principles.....	5
7. Collecting Personal Data	5
8. Sharing personal data.....	6
9. Subject access requests and other rights of individuals	6
10. Parental requests to see the educational record	8
11. Biometric recognition systems	8
12. CCTV	9
13. Photographs and videos	10
15. Data protection by design and default	12
16. Data security and storage of records	12
17. Disposal of records	13
18. Personal data breaches	13
19. Training.....	13
20. Monitoring and review arrangements.....	13
21. Links with other policies	13
Appendix 1: Personal data breach procedure.....	14
Appendix 2: Data Protection Policy statement.....	17
Appendix 3 Data Protection Policy.....	19
Appendix 4 Statutory Requests for Information policy	22
Appendix 5 Acceptable Personal Use of Resources and Assets Policy	24
Appendix 6 Data Handling Security Policy.....	26
Appendix 7 Data Breach Policy	28
Appendix 8 Records Management Policy	29
Appendix 9 Biometrics Policy.....	31

1. 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 General Data Protection Regulation (GDPR) and the expected provisions of the

Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation and guidance

- This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the Information Commissioner's Office (ICO) code of practice for subject access requests.
- It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
- It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.
- In addition, this policy complies with the School Funding Agreement and Articles of Association.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual. This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">• 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	<p>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.</p>

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.

4. The Data Controller

The 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 Information Commissioners Office (ICO) and will renew this registration annually or as otherwise legally required.

5. 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.

5.1 Local Governing Board

The Local Governing Board has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

5.2 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 first point of contact for individuals whose data the school processes is the Data Protection Lead or Senior Information Risk Officer at the school. The school may then refer to the DPO for advice and support.

CCHSG DPO is Information Governance Support and is contactable via Essex County Council, 0333 013 9824.

5.3 Executive Principal

The Executive Principal 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

6. Data Protection Principles

The GDPR is based on data protection principles that the 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.

See Appendix III for the general rules applying to Data Protection Law.

7. Collecting Personal Data

7.1 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 its 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 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 special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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.

7.2 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.

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.

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 record retention schedule & records management policy.

8. 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
- 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 agreement 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 to a country or territory outside the UK we will do so in accordance with data protection law.

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

Subject access requests must be submitted in writing, by letter or email, to the Data Protection Lead or SIRO. They should 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 Data Protection Lead.

9.2 Children and subject access requests

Personal data about a student belongs to that student, and not the student's parents or carers. For a parent or carer to make a subject access request with respect to their student, the student 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 express permission 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- 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

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 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 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 (telephone number 0303 123 1113 or via the ICO website (www.ico.org.uk)).

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 on the basis of public interest
- Request a copy of agreements under which their personal data is transferred anywhere outside 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 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 Data Protection Lead. If staff receive such a request, they must immediately forward it to the Data Protection Lead.

10. Parental requests to see the educational record

Students attending any type of school have a right of access under the Data Protection Act 2018 to their own information. This is known as the right of subject access. When a child cannot act for themselves or the child gives permission, parents will be able to access this information on their behalf.

In academies, including free schools, and independent schools there is no automatic parental right of access to the educational record but may request information via a Subject Access Request.

A request for an educational record must receive a response within 15 school days.

11. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to pay for school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school meals by using a number code.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site for several reasons, namely building security, public safety and for the prevention and detection of crime. We will adhere to the ICO's code of practice for the use of CCTV and the align to the Camera Commissioners Code of Practice 12 guiding Principles

[Surveillance Camera Code of Practice \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk):

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the ICT Services IT Helpdesk.

For further information, please refer to the Surveillance Management Procedure.

13. 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.

Uses may include:

- Within the school on notice boards and in school magazines, brochures, newsletters, etc.
- On social media (Facebook, X etc.)
- For marketing purposes such as the school website, brochures etc. Marketing photographs may be used until the end of the print run or until the website is updated.
- In the media (newspapers – consent is requested which includes the information that newspapers may be published online)

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will not distribute it further.

When using photographs and videos on social media we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

The above commitments apply to occasions where the school can exercise reasonable control of the situation, including events held outside the school organised by external providers. It is clearly not always possible to stipulate conditions for photography, for example in public places during school visits.

In fulfilling the above commitments, we may:

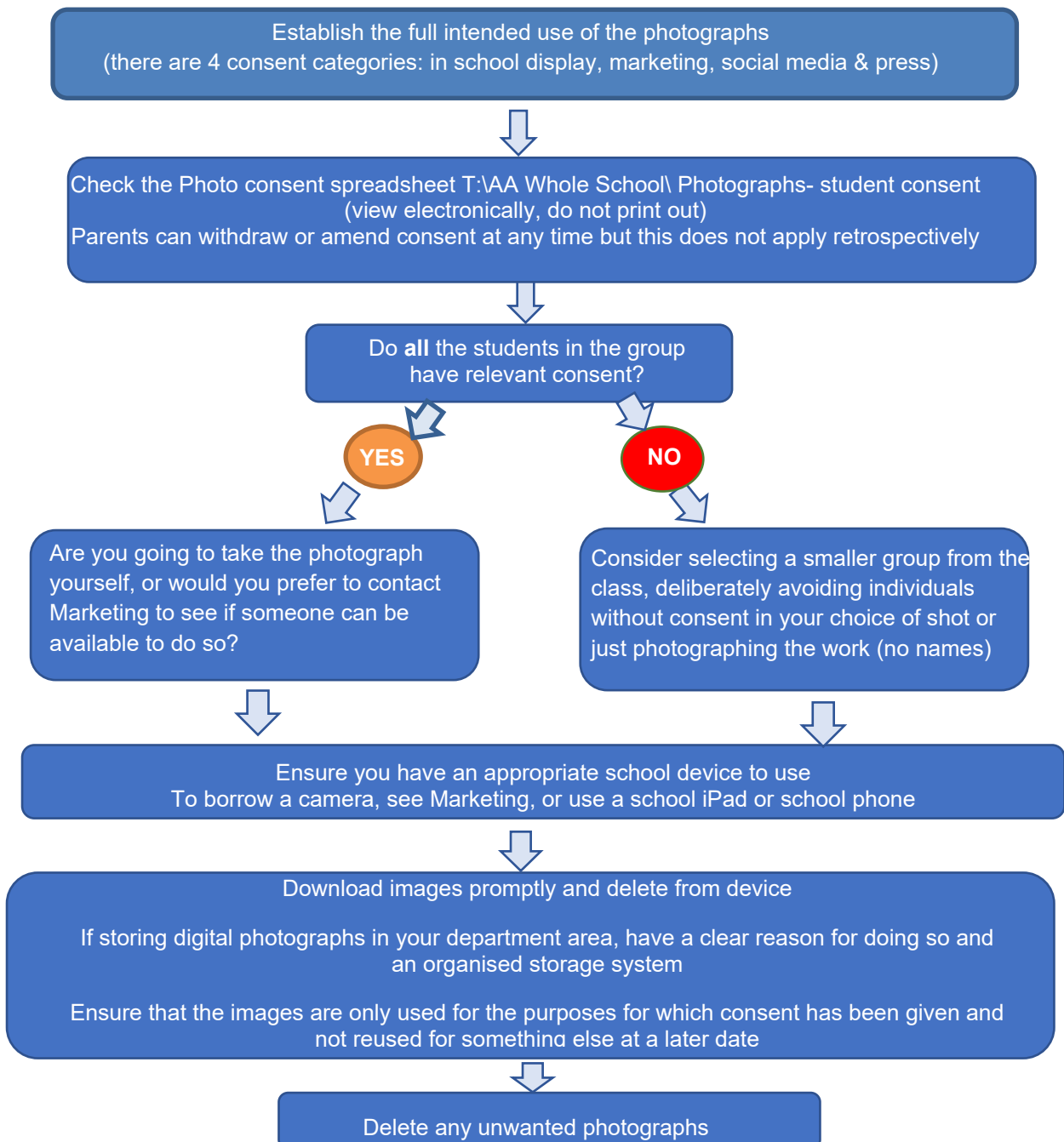
- a) ask parents and others to refrain from photography at events. We will give notice of this in invitations to the events and a notice will be displayed at the event;

- b) make specific exemptions, for example parents/guardians only photographing their child receiving an award, and we will give notice of this in invitations.

If a parent wishes to see specific visual images of their child held by the school, they should make their request to the School Office. At busy times the school may take up to 10 working days to respond to the request.

Where we appoint an official photographer and make arrangements to supply copies of pictures to parents they will be under the same GDPR obligations as the school. See the Alpha Trust Safeguarding & Child Protection Policy (AT2), E-safety Policy (44) and Appendix 6 Data Handling Security Policy for more information on our use of photographs and videos.

Photographing a Student Activity - summary of actions to be taken



15. 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 process 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 privacy 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, how and why we are storing the data, retention periods and how we are keeping the data secure.

16. 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
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our e-Safety Policy and ICT Acceptable Use Agreements Policy 44)
- 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).

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. 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.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

19. 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. An annual update will be provided for staff, usually at the start of the Autumn Term.

20. Monitoring and review arrangements

The Data Protection Lead and SIRO are responsible for monitoring and reviewing this policy. This policy will be reviewed annually and will be reviewed and updated if there are any statutory changes that affect the school's practice.

21. Links with other policies

This Data Protection Policy is linked to:

- AT2 Alpha Trust Safeguarding & Child Protection Policy
- A20 Freedom of information publication scheme
- AT P19 Alpha Trust Code of Conduct
- 44 e-Safety Policy and ICT Acceptable Use Agreement
- 49 Photography in School

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 Data Protection Lead or SIRO
- The Data Protection Lead and SIRO will investigate the report, and determine whether a breach has occurred. To decide, they 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 Data Protection Lead will alert the SIRO and Executive Principal who will inform the Chair of Governors
- The Data Protection Lead and SIRO 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 Data Protection Lead and SIRO will assess the potential consequences, based on how serious they are, and how likely they are to happen. They may need to seek advice from the DPO.
- The Data Protection Lead and SIRO will work out whether the breach must be reported to the ICO, with advice from the DPO. This must be judged on a case-by-case basis. To decide, they 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

If it is likely that there will be a risk to people's rights and freedoms, the Data Protection Lead must notify the ICO.

The Data Protection Lead 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 by the Data Protection Lead.

- Where the ICO must be notified, the Data Protection Lead will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the following will be 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 Data Protection Lead
- 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 Data Protection Lead will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to have further information. The Data Protection Lead will submit the remaining information as soon as possible
- The Data Protection Lead and SIRO will assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. They may need to seek advice from the DPO. If the risk is high, the Data Protection Lead will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the Data Protection Lead and 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 Data Protection Lead 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 Data Protection Lead 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 by the Data Protection Lead.

The Data Protection Lead and Executive Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible after the event.

Breaches of Information Policies will always be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against the staff member responsible.

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) for example:

- *If special category data (sensitive information) is accidentally made available via email to un-authorized 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 Data Protection Lead as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the Data Protection Lead will ask the IT Department to recall it*
- *In any cases where the recall is unsuccessful, the Data Protection Lead will contact the relevant un-authorized 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*
- *The Data Protection Lead will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The Data Protection Lead will carry out an internet search 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*

Other examples of breaches which will need mitigating action

- *Non-anonymised student exam results or staff pay information being shared with school governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen.*

Appendix 2 to Appendix 9 Information Governance Framework

The school follows the Information Governance Framework, and therefore has adopted the following policies and strategies associated with this scheme, as Appendices to our Data Protection Policy.

Appendix 2

Data Protection Policy Statement (For publication on school website)

This policy sets out how we will protect personal data, special category data and criminal convictions personal data.

It meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018.

Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

We ensure that processing is fair by providing detailed privacy notices to individuals whose personal data is being processed. All individuals are advised of their right to contact the Data Protection Officer with any queries regarding the processing of their personal data. We will only process personal data fairly, and will not mislead individuals about how their data may be used.

Principle 2 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

We meet this obligation by explaining through our privacy notices which legal basis we are relying on when processing personal data. We will only use the data for the purposes for which it was collected unless we advise individuals, prior to any additional use, of our intentions and the rights they have in relation to any further use.

Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

We meet this obligation by only collecting what is required for a particular purpose, and ensuring that we have sufficient relevant information for that purpose.

Principle 4 – Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

We meet this obligation by ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.

Principle 5 – Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will

be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

We meet this obligation by ensuring that personal data is managed in line with our retention schedule, and either deleted or completely anonymised when it is no longer necessary for us to use it. The period for which we retain personal data is explained in each privacy notice relevant to that service.

Principle 6 – Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

We meet this obligation by ensuring that our technical and organisational controls are monitored. Our organisational controls include:

- *Appropriate roles and responsibilities including a Data Protection Officer and Senior Information Risk Owner*
- *Robust policies and procedures which are regularly reviewed*
- *Regularly training our staff in their data protection responsibilities*
- *Ensuring our processing activities are transparent and secure, including*
 - *Records of Processing Activities*
 - *Data Protection Impact Assessments*
- *Contractual Controls to govern the use of personal data by our suppliers*
- *Physical security controls including*
 - *Restricted access to physical storage of sensitive personal data*
 - *Visitor management*
- *Security breach management*

Our Technical Controls include:

- *Firewalls, anti-malware and patching*
- *Disaster Recovery and Business Continuity arrangements*
- *Role based access controls to personal data*
- *Password management*
- *Sending email securely*

Principle 7 - The controller shall be responsible for, and be able to demonstrate, compliance with the principles

We meet this obligation by maintaining Records of Processing Activities which are available on demand to the Information Commissioner. We routinely carry out Data Protection Impact Assessments for any processing of special categories of data or where there is a high risk to individuals' privacy. We have appointed a Data Protection Officer and have defined policy and process to manage the exercising of data subjects' rights.

For further information about how we process personal data please see our online privacy notices on our website or contact the Data Protection Lead at the school.

Appendix 3 Data Protection Policy

Data protection is a legal requirement and is vitally important for ensuring that the data of our students, parents/carers, and those that work with the school is kept secure. This will protect the rights of individuals, and ensure that the risks of data processing are well managed.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow when processing personal data.

Policy rules:

1. All employees must **comply** with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals
2. Where personal data is used, we must make sure that the data subjects have access to a complete and current **Privacy Notice**.
3. We must formally **assess** the risk to privacy rights introduced by any new (or change to an existing) system or process which involves the use of personal data, by completing a Data Protection Impact Assessment (DPIA)
4. We must process only the **minimum** amount of personal data necessary to deliver services.
5. All employees who record **opinions** or intentions about students, parents/carers or staff must do so carefully and professionally, distinguishing between fact and opinion.
6. We must take reasonable steps to ensure the personal data we hold is **accurate**, up to date and not misleading.
7. We must rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition
8. Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services, unless you have statutory duties to promote them.
9. Consent will **expire** at the end of each 'Key Stage' period unless it is reconfirmed.
10. We must ensure that the personal data we process is reviewed and **destroyed** when it is no longer necessary.
11. If we receive a **request** from a member of the public or colleague asking to **access** receive a copy of their personal data, we must handle it as a Subject Access Request under the Data Protection Act 2018 or a request for the Education Record under the Education (Pupil Information) (England) Regulations 2005
12. If we receive a request from anyone asking to access the personal data of **someone other than themselves**, we must fully consider Data Protection law before disclosing it
13. When someone contacts us requesting we change the way we are processing their personal data, we must fully consider their **rights** under Data Protection law.
14. You must not access personal data which you have **no right to view**
15. You must follow system user **guidance** or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so
16. You must only **share** personal data with external bodies who request it if there is a current agreement in place to do so or it is approved by the Data Protection Officer (DPO) or Senior Information Risk Owner (SIRO)
17. Where the content of telephone calls, emails, internet activity and video images of employees and the public is **recorded, monitored and disclosed** this must be done in compliance with the law and the regulator's Code of Practice. This activity is considered to be surveillance.
18. All employees must be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely. This training must be regularly refreshed to ensure knowledge remains current.
19. When using '**data matching**' techniques, this must only be done for specific purposes in line with formal codes of practice, informing students, parents/carers or staff of the details, their legal rights and getting their consent where appropriate.

20. We must pay an annual Data Protection Fee
21. Where personal data needs to be anonymised or pseudonymised, for example for **research purposes**, we must follow the relevant procedure and statutory guidance.
22. You must not **share** any personal data held by us with an individual or organisation based in any country outside of the United Kingdom without seeking advice from the SIRO or Data Protection Officer
23. We must identify **Special Categories** of personal data and make sure it is handled with appropriate security and only accessible to authorised persons
24. When **sending** Special Category data to an external person or organisation, it should be marked as "OFFICIAL-SENSITIVE" and where possible, sent by a secure method
25. When considering the use of **artificial intelligence** involving the using or creation of personal data you can only do so on approval from the DPO and SIRO.

How must I comply with these policy rules? All Framework documents can be found:
T:\AA Whole School\GDPR Information Framework 2025

We have related policies, procedures and guidance which tell you how to comply with these rules. These include:

- Statutory Requests Policy (Appendix 4)
- Data Handling Security Policy (Appendix 6)
- Data Breach Policy (Appendix 7)
- Records Management Policy (Appendix 8)
- Biometrics Policy (Appendix 9)
- Privacy Notice Procedure (Website)
- Data Protection Rights Procedure (F6. Framework document)
- Publishing for Transparency Procedure (D11. Framework document)
- Consent Procedure (D3. Framework document)
- Minimisation of Personal Data Procedure (D4. Framework document)
- Data Breach Procedure (D6. Framework document)
- Data Sharing Procedure (D12. Framework document)
- Subject Access Request Procedure (Website)
- Marketing Procedure (Website)
- Surveillance Procedure (D5. Framework document)
- Retention Schedule (D8. Framework document)
- Training & Awareness Procedure (D10. Framework document)
- Statutory Requests for Information Guidance (Appendix 4)
- Overseas Transfers & Hosting Guidance (E9. Framework document)
- 44d Generative Artificial Intelligence Policy

If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018 (including the UK General Data Protection Regulation)
- Article 8, The Human Rights Act 1998
- Education (Pupil Information) (England) Regulations 2005
- Investigatory Powers Act 2016
- Privacy and Electronic Communications Regulations 2003
- The Equality Act 2010

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 4 Statutory Requests for Information policy

It is a legal requirement for all schools to comply with the Freedom of Information Act 2000 (FOI), the Environmental Information Regulations (EIR), the UK General Data Protection Regulations, the Data Protection Act 2018, and the Education (Pupil Information) (England) Regulations 2005.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow when managing these statutory requests for information.

Policy rules:

1. We must **correctly identify** the law which applies to the information being requested and manage the request in compliance with that law
2. Information should be **released** unless there is a strong legal justification for withholding it.
3. Whenever we **refuse** to provide information, we must clearly and fully explain the reasons why
4. We must provide **advice and assistance** to people making a request.
5. We must always try to **reply** as quickly as possible, but always within the legal deadline.
6. All employees must promptly **provide** all relevant information to a request co-ordinator if asked for it
7. If we decide to **charge** for information, we must do so in accordance with a published policy.
8. Where reasonable and practical, we must provide the information in the **format** requested by the requester.
9. When we respond to a request, we must tell the requestor about our **internal review** process.
10. When responding to a complaint, we must advise the requestor that they may **complain to the Information Commissioner's Office (ICO)** if they remain unhappy with the outcome.
11. We must maintain an up-to-date **Publication Scheme** available on our website to meet our obligations under FOI/EIR

How must I comply with these policy rules?

We have related policies, procedures and guidance which tell you how to comply with these rules. These include:

- Records Management Policy (Appendix 8)
- Data Protection Rights Procedure (F6. Framework document)
- Publishing for Transparency Procedure (D11. Framework document)
- Subject Access Request Procedure (Website)
- FOI – EIR Procedure (F7. Framework Document)
- Statutory Requests for Information Guidance (Appendix 4)
- Retention Schedule (D8. Framework document)

All Framework documents can be found: T:\AA Whole School\GDPR Information Framework 2025.

If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018 / UK GDPR
- Freedom of Information Act 2000
- Environmental Information Regulation 2005
- Education (Pupil Information) (England) Regulations 2005

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 5 Acceptable Personal Use of Resources and Assets Policy

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. It is reasonable to assume that at times, staff may use our IT and other facilities resources for personal reasons. However, it is important that boundaries are set to ensure that this is done effectively so that our reputation is maintained and staff working time is used efficiently on delivering our business outcomes.

This policy sets out the rules all staff, governors, contractors and volunteers must follow when using resources and assets provided by the school, including IT facilities, for personal use. It aims to ensure that everyone understands their professional responsibilities when using any form of ICT. All users of ICT need to comply with the Acceptable Use Policy (Appendix 10 44a).

Policy rules:

1. You must use our facilities **economically**; your personal use must not create extra costs for us
2. You must not use our facilities to undertake any unlawful, libellous, immoral or offensive **activities**, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material
3. Personal use must not interfere with your **productivity** and how you carry out your duties
4. Personal use must not reflect adversely on our **reputation**
5. You must not leave **personal-use websites** open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them
6. You must not use browsers or access/ attempt to access sites that are knowingly **unacceptable**, even if this is in your own time
7. You must not **send or forward** chain, joke or spam emails
8. You must not use the Organisation's facilities for **commercial purposes** not approved by us or for personal financial gain
9. You must not use your access rights or identity as an employee to **mislead** another person, for personal gain or in any other way which is inconsistent with your role
10. You must not **disclose** (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it
11. When you print, photocopy or scan official-sensitive information, you must not leave the information **unattended**
12. You must not **connect** any equipment to our IT network that has not been approved
13. You must not do anything that would **compromise** the security of the information held by us. This includes downloading or opening files from an unknown or untrusted source as these may introduce a virus or malware; or disabling or changing standard security settings.
14. You must not make personal use of the information available to you that is not available to the **public**

How must I comply with these policy rules?

By complying with the policy rules set out above and checking with your manager when you have any uncertainty over what is appropriate. We have related policies, procedures and guidance which will help you how to comply with these rules. These include:

- Data Handling Security Policy (Appendix 6)
- Data Breach Policy (Appendix 7)

- Records Management Policy (Appendix 8)
- Data Breach Procedure (Appendix 7)
- Retention Schedule (D8. Framework document)
- E Safety (Policy 44)

All Framework documents can be found: T:\AA Whole School\GDPR Information Framework 2025.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018 / UK GDPR
- Computer Misuse Act 1990

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 6 Data Handling Security Policy

You are the custodian of the equipment and data issued to you to carry out your role; it is your responsibility to keep it physically secure.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow when managing IT equipment, removable storage devices and papers, in the office, in transit and at home or other work locations.

Policy rules:

1. You must take **responsibility** for the security of the equipment allocated to you and that is in your custody.
2. When you are physically **transporting** our data outside of our premises, on any medium, you must take steps to keep it secure
3. You must not leave Official-Sensitive data unattended in a **vehicle** for longer than 10 minutes, and always keep it out of sight
4. You must take appropriate steps to secure our data when working at **home** or other organisations' **premises**
5. If working with our data on approved unmanaged equipment (personal devices), you must **remove** the data when finished, including from cloud storage, and prior to leaving the school's employment
6. If you are taking Official-Sensitive information out of the school, this must be **recorded**
7. You must make sure that conversations discussing sensitive data are only audible by an **appropriate audience**
8. You must not allow anyone to **access** to your IT equipment through your IT account
9. You must not store our business data on any equipment, including personal devices, which has not been **approved**
10. You must not allow unauthorised people to be able view information on your IT equipment **display**
11. You must not save your **passwords** to any web-based system which holds our data in the browser
12. You must always use an approved secure method of **disposing** of physical documents and data storage devices
13. You must **return** all equipment which has been issued to you by us, prior to leaving your employment
14. You must **report** as quickly as possible if your equipment is lost or stolen and assist with any **investigation**
15. You must ensure that all security functions are **enabled** on your portable equipment, such as pin codes and password access
16. You must keep your portable equipment, **clean and serviceable**, including keeping it charged
17. You must not take any of our equipment **abroad** unless you are traveling in a business capacity with approval
18. You must not give your portable equipment to **another person** if you are not using it.
19. You must immediately raise as a **data breach** any loss, unlawful access or theft of the data we are responsible for
20. You must not use new technology that collects personal data (e.g. learning platforms, apps etc) before it has been assessed by completion of a Data Protection Impact Assessment (DPIA)
21. You must add delegates to your email account, so that your business emails can always be accessed when you are on leave. This does not apply to standard leave for staff such as the School Holidays but does apply to any other type of leave such as Annual Leave. ICT Services manage access to accounts and will provide access on approval by the Associate Principals or Executive Principal.

How must I comply with these policy rules?

We have related policies, procedures and guidance which help you comply with these rules. These include:

- Data Protection Policy (Appendix 3)
- Data Breach Policy (Appendix 7)
- Records Management Policy (Appendix 8)
- Data Breach Procedure (D6. Framework document)

All Framework documents can be found: T:\AA Whole School\GDPR Information Framework 2025.

If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

Reference

- Data Protection Act 2018 / UK GDPR
- Article 8, The Human Rights Act 1998

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 7 Data Breach Policy

Handling data breaches appropriately allows us to respond effectively when something has gone wrong. Capturing all types of data breaches, whether it is a confirmed breach, a potential breach or a 'near-miss', allows us to understand where our weaknesses are, how well our policies are working and what we should change about our policies to make them more effective. It allows us to meet our legal obligation to report breaches which may cause harm to individuals to the regulator.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow to effectively manage data breaches.

Policy rules:

1. If you discover a data breach, you must immediately **report** it to the Data Protection Lead
2. When reporting the breach, you must **provide** as much information as possible
3. The Investigating Officer must **complete** investigations and complete an outcome report which can be found in our Data Breach Procedure
4. All staff must support investigations into breaches as required
5. Maintain a full **record** of each breach from reporting to closure
6. The Principal/Senior Information Risk Owner (SIRO) must support the investigation of **major and critical** breaches
7. Comply with the timescales and escalation process outlined in our Data Breach Procedure
8. Major and critical breaches must be referred to the Data Protection Officer.

How must I comply with these policy rules?

Our Data Breach Procedure tells you how to comply with these rules. If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018 / UK GDPR

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 8 Records Management Policy

It is important that school information is managed in compliance with the law and in line with best practice; ensuring the efficient use of resources and lawful data sharing to support efficient business processes and maintain effective service delivery.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow to support secure access and effective retention, destruction, and preservation processes

Policy rules:

1. You must **document** your work activities in line with procedures
2. You must store all work information in the format and **medium** best suited to its use in line with procedures
3. You must ensure that the information you manage is only known to an **appropriate audience**
4. All information in any format which we hold as a record of our activity must be **retained** after 'closure' in line with Retention Guidelines
5. Owners must regularly **review** information in line with Retention Guidelines to make best use of the available storage space
6. We must **monitor** the success of the review process to maintain compliance with the law
7. You must manage pupil records in line with the Retention Guidelines and specific system **guidance**
8. You must follow school policy when storing **emails** as records
9. We must ensure that the **facilities** available for storing and managing information meet legal requirements and best practice
10. We must maintain a **selection procedure** for identifying, reviewing and managing records with **historical value**
11. You must not store business information on a **personal drive** or on equipment not provided by the school
12. All Information **Assets** identified on the Register must be associated with a retention period from the Retention Guidelines.
13. The Retention Guidelines must be reviewed for **changes** in legislation and the school's business needs.
14. When archiving paper records, information on ownership, retention and indexing quality must be recorded.
15. Do not use the archive storage services of any commercial company other than the **approved supplier**
16. Personal information processes must be recorded in your **Records of Processing Activity** (ROPA)

How must I comply with these policy rules?

We have related policies, procedures and guidance which tell you how to comply with these rules. These include:

- Data Protection Policy (Appendix 3)
- Statutory Requests Policy (Appendix 4)
- Data Handling Security Policy (Appendix 6)
- Data Breach Policy (Appendix 7)
- Biometrics Policy (Appendix 9)
- Data Protection Rights Procedure (F6. Framework document)
- Publishing for Transparency Procedure (D11. Framework document)
- Consent Procedure (D3. Framework document)
- Minimisation of Personal Data Procedure (D4. Framework document)
- Data Breach Procedure (D6. Framework document)

- Data Sharing Procedure (D12. Framework document)
- Subject Access Request Procedure (Website)
- Surveillance Procedure (D5. Framework document)
- Retention Schedule (D8. Framework document)
- Statutory Requests for Information Guidance (Appendix 4)
- Overseas Transfers & Hosting Guidance (E9. Framework Document)

All Framework documents can be found: T:\AA Whole School\GDPR Information Framework 2025.

If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018 / UK GDPR
- Article 8, The Human Rights Act 1998
- Freedom of Information Act 2000.
- Code of Practice on Records Management (under Section 46 of the FOI)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 9 Biometrics Policy

A biometric recognition system obtains or records information about a person's physical or behavioural characteristics and compares that information with information which has been previously stored to determine whether the person is recognised by the system. The following rules are necessary to ensure that we comply with data protection law and protect the rights of individuals. They ensure that the risks of data processing are well managed.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow when collecting and managing biometric information.

Policy rules:

1. You must complete a **Data Protection Impact Assessment (DPIA)** for the use of biometric data.
2. The DPIA must be approved by the **Data Protection Officer** prior to the system being used.
3. You must refer to your use of biometric data in your **privacy notices**, ensuring individuals are clear about their rights in relation to its use
4. You must ensure that all students understand that they can **object** or refuse to allow their biometric data to be taken/used
5. You must **gain consent** in writing from at least one parent. ~~Consent is not required from the student, even if they are aged 12 or over (but see point 11)~~
6. You must **document** that consent has been given
7. You must provide a simple process to **object** and **withdraw consent**
8. You must **document** if consent is withdrawn, or objections are raised
9. You must not continue to hold or use biometric data where consent for its use has been **withdrawn**
10. You must ensure that any Biometric data is securely destroyed when no longer used
11. If any parent/guardian/carer withdraws consent, you must **cease** to hold and use the biometric data even if the other parent/guardian/carer has not withdrawn consent
12. You must accept the view of the **student** if they do not want their biometric data used by the school, regardless of their age. The student's wishes supersede any parent/guardian/carer wishes. If both or either parent has consented and the student does not wish the data to be processed, the student's wishes take precedent.
13. You must ensure that there is an **alternative arrangement** available for any services which use biometrics
14. Ensure that biometric data is held in an encrypted form, and that all available technical and organisational **security** measures are applied
15. Your use of biometric data must be recorded in your **records of processing activities (RoPA)** (Framework document H1)
16. You must not share biometric data with 3rd parties unless there is an **appropriate contract** in place protecting the rights of data subjects

How must I comply with these policy rules?

We have related policies, procedures and guidance which tell you how to comply with these rules. These include:

- Data Protection Policy (Appendix 3)
- Data Handling Security Policy (Appendix 6)
- Data Breach Policy (Appendix 7)
- Records Management Policy (Appendix 8)
- Data Protection Rights Procedure (F6. Framework document)
- Consent Procedure (D3. Framework document)
- Data Breach Procedure (D6. Framework document)

- Subject Access Request Procedure (Website)
- Surveillance Procedure (D5. Framework document)
- Retention Schedule (D8. framework document)

All Framework documents can be found: T:\AA Whole School\GDPR Information Framework 2025.

If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

References

- Data Protection Act 2018 / UK GDPR
- Article 8, The Human Rights Act 1998
- Protection of Freedoms Act 2012
- [ICO Biometric data guidance](#)
- DfE - [Protection of biometric information of children in schools and colleges – July 2022](#)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.