Fareham Academy

Data Protection Policy

March 2026

Date Approved:	**March 26**	Review Date:	**March 27**	Approved by:	**The Trust Board**

1 Aims

Fareham Academy aims to ensure that all personal data collected about staff, pupils, parents, Trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

2 Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

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 guidance for the use of surveillance cameras and personal information.

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

3 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership

	• Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4 The Data Controller

Fareham Academy processes personal data relating to parents, pupils, staff, Trustees, visitors and others, and therefore is a data controller.
The Academy is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

1. Roles & Responsibilities

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

5.1 The Trust Board

The Trust Board has overall responsibility for ensuring that the Academy complies with all relevant data protection obligations.

1.2 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 Body and, where relevant, report to the Trustees their advice and recommendations on school data protection issues.
The DPO is also the first point of contact for individuals whose data the Academy processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.
Our DPOs are Misss C Roberts & Mrs N Knight and they are contactable via email:
dpo@fareham-academy.co.uk

1.3 Headteacher

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

1.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy and taking due care when working on electronic devices outside of school
- Informing the Academy 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 European Economic Area
    - 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

5 Data Protection Principles

The Academy processes personal data in accordance with the principles in Article 5 UK GDPR. Personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purpose**s** (with statutory exceptions for archiving in the public interest, scientific or historical research, or statistical purposes);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for those purposes;
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
- Accountability: The Academy is responsible for, and able to demonstrate compliance with, all the above principles.

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

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 Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy 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 Academy, as a public authority, can perform a task in the public interest, and carry out its official functions. The Academy will rely on **public task** as the lawful basis for most of its processing. As a public authority, we process personal data where this is necessary for us to perform a task carried out in the public interest or to exercise our official functions, including our statutory duties under education and safeguarding legislation. This is the primary lawful basis for the majority of our day-to-day processing of pupil, parent, and staff information.
- The data needs to be processed for the legitimate interests of the Academy or a third party (but only for activities that do not form part of the Academy's official public tasks. As a Public Authority, the Academy can not rely on legitimate interests for processing that it carries out in the performance of its statutory functions. We will therefore only use legitimate interests for option, non-core activities where individuals would reasonably expect such processing and where their rights and freedoms are not overridden),
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent

- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them. We only process special category or criminal offence data where it is strictly necessary, proportionate, and supported by the relevant condition under the UK GDPR or the Data Protection Act 2018.

7.2 Limitation, minimisation and accuracy

We will collect personal data only for specified, explicit and legitimate purposes, and we will explain those purposes to the individuals at the point of collection via our applicable privacy notices.

If we wish to use personal data for a new purpose, we will first assess whether the new purpose is compatible with the original purpose under the UK GDPR. Where the new purpose is not compatible, we will identify and document a new lawful basis (which may, in some cases, be consent) before proceeding, and we will provide updated privacy information as required.

Staff must only process personal data where it is adequate, relevant and limited to what is necessary for their role. We will implement appropriate technical and organisational measures to enforce this.

We will keep personal data accurate and, where necessary, up to date, and will take every reasonable step to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is rectified or erased without delay.

Personal data will be retained only for as long as necessary for the purposes for which it was collected and will then be securely deleted or truly anonymised (rendered irreversibly non-identifiable). Retention and disposal will follow the Academy's records retention schedule.

6 Sharing Personal Data

We will not normally share personal data with anyone else. We may share personal data where it is lawful and necessary to do so, including in the following circumstances:

- Where there is a concern for the safety of staff, pupils or others (vital interests or public task).
- Where we need to liaise with other agencies (for example, safeguarding partners, the local authority, NHS services or social care) in order to fulfil our statutory responsibilities. We will identify the appropriate lawful basis for such sharing. Consent will only be used where no lawful basis applies.
- Where our suppliers or contractors require access to personal data to enable us to provide services to the Academy – for example, IT providers and educational platforms. In these cases we will:
    - Only use suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Put in place a UK GDPR-compliant Data Processing Agreement in the contract;
    - Share only the minimum data necessary for them to provide the service and ensure appropriate safeguards.

We will also share personal data where we are legally required to do so, including law enforcement or 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;
- Compliance with Court Orders or legal proceedings;
- Meeting safeguarding obligations.

We may also share data for research and statistical purposes, where the information is fully anonymised, or where a lawful basis (and where needed consent) applies.

We may also share personal data with emergency services or local authorities where necessary to respond to an emergency involving pupils or staff.
Where personal data is transferred outside the EEA/UK, we will ensure that an adequacy decision or appropriate safeguards, such as Standard Contractual Clauses, are in place in line with UK GDPR requirements.

7 Subject access requests and other rights of individuals

7.2 Subject access requests

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

- Confirmation that we process their personal data;
- Access to a copy;

And the supplementary information required by Article 15 UK GDPR:

- The purposes of the data processing
- The categories of personal data concerned
- The recipients or categories of recipients

- The retention period/criteria,
- The source of the data, if not the individual
- Details of any automated decision-making, including profiling.

We will provide responses in a concise, intelligible form and disclose information securely; where feasible we will respond electronically if requested.

How to make a request
A SAR can be made verbally or in writing (including via social media) to any member of staff. Staff must recognise a SAR and forward it to the DPO immediately. To help us respond promptly, requesters are encouraged to provide: name, contact details, and a clear description of the information sought

Identity and clarification
We may reasonably ask for two forms of ID where necessary to verify identity. Where we process large volumes of information, we may ask the requester to clarify scope; in some circumstances we may pause the one-month time limit until we receive the ID/authority or necessary clarification.

9.2 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 pupils at the Academy may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

We will respond without undue delay and within one month of receipt. We may extend by up to two further months where requests are complex or numerous; if so, we will inform the requester within one month and explain why. We will not charge a fee unless a request is manifestly unfounded or excessive, or further copies are requested.

We will not disclose information if it:
- Might cause serious harm to the physical or mental health of the pupil 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
- Has been refused by the child and they do not consent to the sharing of their personal data.

If the request is manifestly unfounded or excessive, we may refuse to act on it (in whole or in part) or charge a reasonable fee. If we refuse a request, we will tell the individual why, inform them of their right to complain to the ICO, and their right to a judicial remedy.

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.

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 collect personal data, individuals also have the following rights under the UK GDPR and Data Protection Act 2018:

- The right to withdraw consent at any time, where processing is based on consent. This does not affect the lawfulness of processing carried out before consent was withdrawn.
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

8

10. Parental requests to see the educational record

As an academy, the statutory right for parents to access a child's educational record under the Education (Pupil Information) (England) Regulations 2005 does not apply. Where parents request information about their child, we will handle the request under the UK GDPR and the Data Protection Act 2018—considering the child's age and capacity and, where applicable, any subject access request made by or on behalf of the child. The academy will not charge a fee unless permitted under UK GDPR (e.g., where a request is manifestly unfounded or excessive)

11. Call recording

The Academy has an automatic telephone recording system which records all phone calls made to, or from, the Academy using external lines. External callers will receive an automated message informing them of this fact. Parents/carers have been informed of this recording system through letter; there is also notification on the Academy website via this announcement. We record calls to establish facts in case of complaint or incident, support safeguarding enquiries, evidence service quality and provide limited training and quality assurance. The Academy can access such calls using the telephone management system. Recordings are stored securely with restricted, role-based access and audit logging. Access is granted only where necessary. Recordings are disclosed securely if required by law

enforcement or where otherwise lawful. The system does not record internal phone calls. Recorded calls are held for a 12-month period, please refer to the Call Recording Policy for further information. We have completed a Data Protection Impact Assessment (and periodically review this) covering call recording, including the impact on staff and callers, proportionality and safeguards.

12. Biometric recognition systems

The Academy may use pupils' biometric data as part of an automated biometric recognition system such as fingerprints to provide cashless catering. Where we do so, we will comply with the Protection of Freedoms Act 2012 and data protection law.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Academy 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 pupils have the right to choose not to use the Academy's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. Students will be able to access their accounts using a secure PIN and pay for items without using biometrics. Parents/carers and pupils can object to participation in the Academy's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is securely deleted. Parents/carers and pupils may also withdraw consent to use the payment facility. In this case, they will not be able to purchase items from the canteen.

As required by law, if a pupil 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 pupil's parent(s)/carer(s).

Where staff members or other adults use the Academy'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 Academy will delete any relevant data already captured.

We complete and keep under review a DPIA covering the Biometrics system. Biometric data is stored securely with restricted access and audit controls and is retained only for as long as necessary for the stated purposes before secure deletion.

13. CCTV

We use CCTV in various locations around the Academy site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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.

CCTV footage is retained only for as long as necessary for security and safeguarding purposes, in line with our retention schedule, after which it is securely deleted in accordance with the storage limitation principle.

Parents and other third parties are not permitted to view CCTV footage where doing so would disclose images of individua's other than their child, as this would compromise those individuals' privacy. Any enquiries about the CCTV system should be directed to Mrs C Roberts, Deputy Headteacher & Mrs N Knight, Assistant Headteacher

14. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our Academy. Photographs and videos are classes as personal data when individuals can be identified, and we process them in accordance with the Data Protection Act.

For images that are necessary for the Academy's public tasks (for example pupil identification or safeguarding documentation) we do not require parental consent. For optional uses such as communication, marketing or promotional materials, we will obtain written consent from parents/carers and where appropriate the pupil.
Uses may include:

Consent will be collected with a clear explanation of how photographs and or video will be used. Individuals may refuse or withdraw consent at any time. Where processing is based solely on consent, the Academy will stop using the image and will delete it from future publications. Where photographs or videos are required for core educational or safeguarding purposes under our public task basis, withdrawal of marketing consent does not affect these uses.

In line with best practice, we will not accompany photographs with identifying personal information unless specific consent has been obtained. Parents, carers or pupils may contact the Academy at any time to discuss how their images are being used.

15. Use of Artificial Intelligence (AI)

As part of our aim to reduce staff workload while improving outcomes for our students, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must follow best data protection practices as set out in this policy.
To protect data when using generative AI tools, staff must:

- Use only approved AI tools (primarily Microsoft Copilot)
- Seek advice from the data protection officer and IT Support, as appropriate
- Report safeguarding concerns to the DSL in line with our school's child protection and safeguarding policy
- Ensure there is no identifiable information included in what they put into generative AI tools
- Acknowledge or reference the use of generative AI in their work
- Fact-check all results to make sure the information is accurate and suitable for use

All staff play a role in ensuring that students understand the potential benefits and risks of using AI in their learning. All staff have a responsibility to guide students in critically evaluating AI-generated information and understanding its uses and limitations.

16. 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 privacy impact assessments where the Academy'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 Academy 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

17. 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 pupils 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, pupils or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. All devices must be password protected.
- 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

18. 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 Academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19. Personal data breaches

The Academy takes all reasonable steps to prevent personal data breaches. We maintain breach detection, investigation and internal reporting procedures so incidents are identified, escalated and assessed properly. Staff must report any suspected incident immediately to the DPO.

We will assess the likely risk to individual' rights and freedoms. Where a breach is notifiable, we will report it to the ICO within 72 hours of becoming aware, explaining the nature of the breach, the categories and/or approximate number of data subjects and records concerned, the likely consequence, and the measures taken or proposed. If we do not yet have all details, we will submit the initial notification and provide updates without undue delay.

If the breach is likely to result in high risk to individuals, we will also notify affected individuals without undue delay, providing advice to help them protect themselves (for example password changes, vigilance for phishing, identify fraud). We record all personal data breaches, whether we notify the ICO or not, in a breach register – which includes the facts, effects, remedial actions and our notification decisions with reasons. Where a processor acting on our behalf experiencing a breach, they must notify us without undue delay. We (as controller) will assess the incident and determine any ICO/individual notifications.

Examples of reportable school breaches may include, but are not limited to:

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

The Academy uses the ICO's breach assessment guidance to support decision-making.

20. Training

All staff and Trustees are provided with data protection training as part of their induction process and this is refreshed annually.

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

21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed **every 2 years** and shared with the full The Trust Board for their approval.

The policy may be reviewed earlier is there are significant legal or operational changes.