

Data Protection Privacy Notices Fairfax Multi-Academy Trust

Document Owner:	Robert Fitzgerald, I&S Manager & DPO
Ratified By:	Audit & Risk Committee (ARC)
Date Ratified:	April 2026
Review Date:	September 2027



FMAT Privacy Notices

Contents

Privacy Notice for Applicants **Page 3 to 5**

This privacy notice is for applicants who are applying to a position to work at Fairfax Multi-Academy Trust or an academy within the trust.

Privacy Notice for Parents/Carers **Page 6 to 8**

This privacy notice is for parents or carers of pupils who attend a Fairfax Multi-Academy Trust academy.

Privacy Notice for Students **Page 9 to 11**

This privacy notice is for students who attend a Fairfax Multi-Academy Trust academy.

Privacy Notice for Workforce **Page 12 to 15**

This privacy notice is for current employees of Fairfax Multi-Academy Trust.

Privacy Notice for members/directors/governors **Page 16 to 18**

This privacy notice is for members/directors/governors who are in governance roles at Fairfax Multi-Academy Trust.

Privacy Notice for Alumni **Page 19 to 20**

This privacy notice is for former students who are alumni at Fairfax Multi-Academy Trust.

Protection of Biometric Information **Page 21 to 26**

This is the Trust's protection of biometric information policy which outlines how biometric information is processed and used across the Trust.

Applicants Privacy Notice

1. Privacy notice for applicants

We are Fairfax Multi-Academy Trust. As part of your application to join us, we will gather and use information relating to you. Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from you directly and data about you that we obtain from other people and organisations. We might also need to continue to hold an individual's personal data for a period of time after the recruitment process, even if you are unsuccessful. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will gather and hold about individuals who apply for a position with us, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

2. What information do we process during your application process?

We may collect, hold, share and otherwise use the following information about you during your application process.

- your name and contact details (i.e. address, home and mobile phone numbers, email address);
- details of your qualifications, training, experience, duties, employment history (including job titles, salary, relevant dates and working hours), details of driving licence (if relevant for role), membership of professional bodies and interests;
- your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;
- information regarding your criminal record;
- details of your referees;
- whether you are related to any member of our workforce or students; and
- details of any support or assistance you may need to assist you at the interview because of a disability.
- information about your previous academic and/or employment history, including details of any conduct, grievance or performance issues, appraisals, time and attendance, from references obtained about you from previous employers and/or education providers;*
- confirmation of your academic and professional qualifications (including seeing a originals of certificates);*
- information via the DBS process, regarding your criminal record, in criminal records certificates (CRCs) and enhanced criminal records certificates (ECRCs), whether you are barred from working in regulated activity;*
- your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;*
- medical check to indicate fitness to work;*

- a copy of your driving licence (or other appropriate documentation as listed on the Home Office list);*
- if you are a teacher, we will check the National College of Teaching and Leadership (“NCTL”) Teachers Services about your teacher status, whether you are subject to a prohibition from teaching order and any other relevant checks (for example Section 128 direction for management posts and EEA teacher sanctions);* and
- equal opportunities' monitoring data.

You are required (by law or in order to enter into your contract of employment) to provide the categories of information marked (*) above to us to enable us to verify your right to work and suitability for the position. Without providing us with this information, or if the information is not satisfactory, we will not be able to proceed with any offer of employment.

If you are employed by us, the information we collect may be included on our Single Central Record. In this scenario, a further privacy notice in relation to data we collect, process, hold and share about you during your time with us, will be issued to you.

3. Where do we get information about during your application process?

Depending on the position that you have applied for, we may collect this information from you, your referees (details of whom you will have provided), your education provider, any relevant professional body, the Disclosure and Barring Service (DBS), NCTL and the Home Office, during the recruitment process.

4. Why do we use this information?

We will process your personal data during your application process for the purpose of complying with legal obligations, carrying out tasks which are in the public interest, and taking steps with a view to entering into an employment contract with you. This includes:

- to assess your suitability for the role you are applying for;
- to take steps to enter into a contract with you;
- to check that you are eligible to work in the United Kingdom or that you are not prohibited from teaching; and
- so that we are able to monitor applications for posts in the Trust to ensure that we are fulfilling our obligations under the public-sector equality duty under the Equality Act 2010.

5. How long will we hold information in relation to your application?

We will hold information relating to your application only for as long as necessary. If you are successful, how long we need to hold on to any information will depend on type of information.

If you are unsuccessful, we will hold your personal data only for six months, after which time it is securely deleted and destroyed.

6. Who will we share information with about your application?

We will not share information gathered during your application process with third parties, other than professional advisors such as legal and HR advisors, referees, our applicant tracking system.

7. Rights in relation to your personal data

All individuals have the right to request access to personal data that we hold about them. To make a request for access to their personal data, individuals should contact the Data Protection Officer.

Please also refer to our Data Protection Policy for further details on making requests for access to personal data.

Individuals also have the right, in certain circumstances, to:

- Object to the processing of their personal data
- Have inaccurate or incomplete personal data about them rectified
- Restrict processing of their personal data
- Object to the making of decisions about them taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of their data protection rights

If an individual wants to exercise any of these rights, they should contact the Data Protection Officer. The law does not oblige the Trust to comply with all requests. If the school does not intend to comply with the request, the individual will be notified of the reasons why in writing.

8. Concerns

If an individual has any concerns about how we are using their personal data, we ask that they contact our Data Protection Officer in the first instance. However, an individual can contact the Information Commissioner's Office should they consider this to be necessary, at <https://ico.org.uk/concerns/>.

9. Contact

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer on dpo@fmat.co.uk or by post:

**FAO Data Protection Officer, Fairfax Multi-Academy Trust,
Fairfax Road, Sutton Coldfield,
B75 7JT**

Parent / Carer Privacy Notice

1. Privacy notice for parents/carers

We are Fairfax Multi-Academy Trust, which your Academy is part of. During your child's time with us, we will gather and use information relating to you. Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from you directly and data about you that we obtain from other people and organisations. We might also need to continue to hold your personal data for a period of time after your child has left the Trust. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will hold about you, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

2. What information do we process in relation to you?

We will collect, hold, share and otherwise use the following information about you:

- personal information (such as name, address, home and mobile numbers, personal email address, emergency contact details and relationship marital status)
- financial details (such as bank account or credit card details), and other financial details such as eligibility for free school meals or other financial assistance
- CCTV footage and images obtained when you attend a Trust site
- your relationship to your child, including any Court orders that may be in place

We will also use special categories of data such as gender, age, ethnic group, religious or similar beliefs, information about health and biometric data. These types of personal data are subject to additional requirements.

3. Where do we get your personal data from?

We will obtain an amount of your personal data from you, by way of information gathering exercises at appropriate times such as when your child joins the Trust, and when you attend the Academy site and are captured by our CCTV system.

We may also obtain information about you from other sources. This might include information from the local authorities or other professionals or bodies, including a Court, which might raise concerns in relation to your child.

4. Why do we use your personal data?

We will process your personal data for the following reasons:

1. Where we are required by law, including:
 - To provide reports and other information required by law in relation to the performance of your child
 - To raise or address any concerns about safeguarding
 - To the Government agencies including the police
 - To obtain relevant funding for the Trust
 - To provide or obtain additional services including advice and/or support for your family

2. Where the law otherwise allows us to process the personal data as part of our functions as a Trust, or we are carrying out a task in the public interest, including:
 - To confirm your identity
 - To communicate matters relating to the Trust/Academy to you
 - To safeguard you, our pupils and other individuals
 - To enable payments to be made by you to the Trust/Academy
 - To ensure the safety of individuals on the Trust site
 - To aid in the prevention and detection of crime on the Trust/Academy site
3. Where we otherwise have your consent

Whilst the majority of processing of personal data we hold about you will not require your consent, we will inform you if your consent is required and seek that consent before any processing takes place.

5. Why do we use special category personal data?

We may process special category personal data in relation to you for the following reasons:

1. Where the processing is necessary for reasons of substantial public interest, including for purposes of equality of opportunity and treatment, where this is in accordance with our Data Protection Policy.
2. Where the processing is necessary in order to ensure your health and safety on a Trust site, including making reasonable adjustments for any disabilities you may have.
3. Where we otherwise have your explicit written consent.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests of those of your child, and where it is not possible to seek your consent.

6. Failure to provide this information

If you fail to provide information to us we may be prevented from complying with our legal obligations.

7. How long will we hold your personal data for?

We will hold your personal data only for as long as necessary. How long we need to hold on to any information will depend on the type of information.

8. Who will we share your personal data with?

We routinely share information about you with:

- Local authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes
- The Department for Education and/or the Education and Skills Funding Agency, in compliance with legal obligations of the Trust to provide information about students and parents as part of statutory data collections
- Contractors, such as payment processing providers to enable payments to be made by you to the Trust Government or health agencies such as NHS Test and Trace in the interest of interests of public health

The Department for Education may share information that we are required to provide to them with other organisations. For further information about the Department's data sharing process, please visit: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>.

Contact details for the Department can be found at <https://www.gov.uk/contact-dfe>.

Local authorities may share information that we are required to provide to them with other organisations.

Bournville School, Erdington Academy and Fairfax are part of Birmingham City Council. For further information about Birmingham local authority's data sharing process, please visit: <https://www.birmingham.gov.uk/>

Smith's Wood Academy are part of Solihull Metropolitan Borough Council. For further information about Solihull local authority's data sharing process, please visit: <http://www.solihull.gov.uk/>

9. Your rights in relation to your personal data held by us

You have the right to request access to personal data that we hold about you, subject to a number of exceptions. To make a request for access to your personal data, you should contact the Data Protection Officer.

Please also refer to our Data Protection Policy for further details on making requests for access to your personal data.

You also have the right, in certain circumstances, to:

- Object to the processing of your personal data
- Have inaccurate or incomplete personal data about you rectified
- Restrict processing of your personal data
- Object to the making of decisions about you taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of your data protection rights

If you want to exercise any of these rights, then you should contact the Data Protection Officer. The law does not oblige the Trust to comply with all requests. If the Trust does not intend to comply with the request, then you will be notified of the reasons why in writing.

10. Concerns

If you have any concerns about how we are using your personal data, then we ask that you contact our Data Protection Officer in the first instance. However an individual can contact the Information Commissioner's Office should you consider this to be necessary, at <https://ico.org.uk/concerns/>.

11. Contact

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer at dpo@fmat.co.uk or by post at:

**FAO Data Protection Officer, Fairfax Multi-Academy Trust,
Fairfax Road, Sutton Coldfield, Birmingham,
B75 7JT**

Student Privacy Notice

1. Why are we giving this to you?

As your school we need to use information about you. We do this for a number of reasons. This form tells you what information we use about you and why we use it. It is very important that information about you is kept safe. We explain below how the school keeps your information safe.

If you want to know anything about what we do with information about you then please ask your teacher, or speak to your parents/guardians and ask them to contact the school. The school wants you to feel free to raise any questions at all.

We also have a person called the Data Protection Officer at the school. They can answer any questions you have about what the school does with your information. If you or your parents/guardian want to speak to them, then you can do by emailing dpo@fmat.co.uk or writing to:

**FAO Data Protection Officer,
 Fairfax Multi-Academy Trust,
 Fairfax Road,
 Sutton Coldfield,
 Birmingham,
 B75 7JT**

2. Privacy notice for students

We are Fairfax Multi-Academy Trust, which your academy is part of. During your time with us, we will use information that we gather in relation to you for various purposes. Information that we hold in relation to you is known as "personal data". This will include data that we obtain from you directly and data about you which we obtain from other people and organisations. We might also need to continue to hold your personal data for a period of time after you have left the school. Anything that we do with your personal data is known as "processing".

This document sets out what personal data we will hold about you, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

3. What information do we use about you?

We will collect, hold, share and otherwise use information about you set out in the boxes below:

• Name	• Telephone and email contact details	• Date of Birth
• Address	• Assessment information	• Details of previous/future schools
• Unique pupil number	• Behavioural information	• Language(s)
• Nationality	• Country of birth	• Eligibility for free school meals
• Photographs	• Attendance information	• CCTV images

We will also collect, hold, share and otherwise use some information about you which is special "special category personal data" and we will take extra care to make sure that this is kept safe:

<ul style="list-style-type: none"> • Racial or ethnic origin 	<ul style="list-style-type: none"> • Religious beliefs 	<ul style="list-style-type: none"> • Special educational needs and disability information
<ul style="list-style-type: none"> • Medical / health information / dietary requirements 	<ul style="list-style-type: none"> • Biometric data 	<ul style="list-style-type: none"> • Information relating to keeping you safe

4. Where do we get this information from?

We get this information from:

- You
- Your parents/guardians, and other children's parents/guardians
- Teachers and other staff
- People from other organisations, for example local authority or a doctor

5. Why do we use this information?

We use this information for lots of reasons, including:

- To make sure that we give you a good education and to support you through this
- To make sure that we are able to address and support any educational, health or social needs you may have
- To make sure everyone is treated fairly and equally
- To keep you and everyone at the school safe and secure
- To deal with emergencies involving you
- To celebrate your achievements
- To provide reports and additional information to your parents/carers

Some of these things we have to do by law. Other things we do because we need to so that we can run the school.

Sometimes we need permission to use your information. This includes taking pictures or videos of you to be used on our website or in the newspaper. Before we do these things we will ask you or if necessary your parent/carer for permission.

6. Why do we use special category personal data?

We may need to use the information about you which is special (mentioned above) where there is a specific interest to do so for example health and social care purposes or to provide you with equal opportunities and treatment. We will also use this information where you have given us permission to do so.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests and where you are unable to provide your consent.

7. How long will we hold information in relation to our students?

We will hold information relating to you only for as long as necessary. How long we need to hold on to any information will depend on the type of information. Where you change school we will usually pass your information to your new school.

8. Who will we share student information with?

We may be give information about you with:

- Other schools or educational institutions you may attend or require support from Local Authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes
- The Department for Education as required by the law
- Contractors, to enable them to provide an effective service to the school, such as school meal providers or external tutors

9. Keeping this information safe

It is very important that only people who need to use your information can see it. The school keeps your information safe by following our data protection policy and procedures.

10. Your rights in relation to your information

You can ask to see the information we hold about you. If you wish to do this, you should contact the Data Protection Officer.

You also have the right to:

- Object to what we are doing with your information
- Have inaccurate or incomplete information about you amended
- Ask us to stop doing certain things with your information in some cases
- Ask that decisions about you are not made using automatic systems
- Claim against the school in certain circumstances where you have suffered as a result of the school breaching your data protection rights

If you feel it necessary to do any of the above, you can speak with the Data Protection Officer. The school does not have to meet all of your requests and we will let you know where we are unable to do so.

11. Concerns

If you are concerned about how we are using your personal data then you can speak with the Data Protection Officer, or if necessary you or your parent/ carer can contact an outside agency - the Information Commissioner's Office who could also help at <https://ico.org.uk/concerns/>.

Workforce Privacy Notice

1. Privacy notice for the workforce

During an individual's employment with Fairfax Multi-Academy Trust, we will use information that we gather in relation to them for various purposes. Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from the individual directly and data about the individual that we obtain from other people and organisations. We might also need to continue to hold an individual's personal data for a period of time after they have left the Trust. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will hold about our workforce, why we process that data, who we share this information with, and the rights of individuals in relation to their personal data processed by us.

2. What information do we process in relation to our workforce?

We will collect, hold, share or otherwise use the following information about our workforce:

- personal information (such as name, address, home and mobile numbers, personal email address, employee or teacher number, national insurance number, and emergency contact details)
- contractual information (such as start dates, hours worked, post, roles and salary information, bank/building society details)
- work absence information (such as number of absences and reasons (including information regarding physical and/or mental health), holiday records)
- qualifications / training courses attended and, where relevant, subjects taught (such as training record)
- performance information (such as probation records, appraisals and performance reviews, performance measures including performance management/improvement plans, disciplinary or grievance records)
- other information (such as pension arrangements (and all information included in these necessary to administer them), time and attendance records, information in applications made for other posts within the Trust, criminal records information (including the results of Disclosure and Barring Service (DBS) checks), details in references the Trust receives or provides to other organisations, CCTV footage and images)

We may also use special categories of data including such as gender, age, ethnic group, sex or sexual orientation, religious or similar beliefs, trade union membership, information about health and biometric data. These types of personal data are subject to additional requirements.

3. Where do we get information from about our workforce?

A lot of the information we have about our workforce comes from the individuals themselves. However, we may also obtain information from tax and regulatory authorities such as HMRC, previous employers, your trade union, the DBS, our insurance benefit administrators, consultants and other professionals we may engage, recruitment or vetting agencies, other members of staff, students or their parents, and publicly available resources including online

sources. In addition, we may obtain information from automated monitoring of our websites and other technical systems such as our computer networks and systems, CCTV and access control systems, communications systems, remote access systems, email and instant messaging systems, intranet and internet facilities, telephones, voicemail and mobile phone records.

4. Why do we use this information?

We will process the personal data of our workforce for the following reasons:

1. Where we are required by law, including:
 - To comply with the law regarding data sharing (see further below)
 - To comply with specific employment law requirements, including our obligations as an employer under employment protection and health and safety legislation, and under statutory codes of practice such as those issued by ACAS
 - To comply with legal requirements in relation to equalities and non-discrimination
2. Where we are required by any contract with our workforce, such as employment contracts, including:
 - To make payments to our workforce, such as salary payments
 - To deduct tax and National Insurance contributions
 - To make a decision about recruitment
 - To check individuals are legally entitled to work in the UK
 - Administering employment contracts
 - Conducting performance reviews
 - Making decisions about salary and compensation
 - Liaising with pension providers
3. Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest, including:
 - To enable the development of a comprehensive picture of the workforce and how it is deployed
 - To inform the development of recruitment and retention policies
 - To safeguard our pupils and other individuals
 - To ensure safe working practices
 - In the interests of ensuring equal opportunities and treatment
 - To administer our employee benefits platform

4. Where we otherwise have the consent of the individual

Whilst the majority of processing of personal data of our workforce will not require consent, we will inform individuals if their consent is required and seek that consent before any processing takes place. Due to the imbalance of power in an employee to employer relationship, it is generally thought that although consent may be implied it cannot truly be freely given. So consent is not necessarily the most appropriate basis to rely upon as an employer.

5. Why do we use special category personal data?

We may process special category personal data of our workforce for the following reasons:

1. To carry out our legal obligations in relation to employment law, where this is in accordance with our Data Protection Policy.
2. Where the processing is necessary for reasons of substantial public interest, including for purposes of equality of opportunity and treatment, where this is in accordance with our Data Protection Policy.
3. For the purposes of preventative or occupational medicine in order to assess an individual's working capacity and/ or the need for reasonable adjustments.
4. Where we otherwise have an individual's explicit written consent – subject to the restriction set out above on the use of consent in an employment relationship.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests and where you are unable to provide your consent.

6. Failure to provide this information

If our workforce fails to provide information to us, this may result in us being unable to perform the employment contract, or we may be prevented from complying with our legal obligations.

7. How long will we hold information in relation to our workforce?

We will hold information relating to our workforce only for as long as necessary. How long we need to hold on to any information will depend on the type of information.

8. Who will we share information with about our workforce?

We routinely share information about our workforce with:

- Local authorities to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes
- The Department for Education in compliance with legal obligations of the school to provide information about our workforce as part of statutory data collections
- Contractors, such as payroll providers, to enable them to provide an effective service to the school and government agencies such as HMRC and DWP regarding tax payments and benefits
- Our professional advisors including legal and HR consultants
- Government or health agencies such as NHS Test and Trace in the interest of interests of public health

- Third parties such as our HR systems and our Health and Safety Systems.

The Department for Education may share information that we are required to provide to them with other organisations. For further information about the Department's data sharing process, please visit: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>.

Contact details for the Department can be found at <https://www.gov.uk/contact-dfe>.

9. Rights of our workforce in relation to their personal data

All of our workforce have the right to request access to personal data that we hold about them. To make a request for access to their personal data, individuals should contact the Data Protection Officer.

Please also refer to our Data Protection Policy for further details on making requests for access to workforce information.

Individuals also have the right, in certain circumstances, to:

- Object to the processing of their personal data
- Have inaccurate or incomplete personal data about them rectified
- Restrict processing of their personal data
- Object to the making of decisions about them taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of their data protection rights

If an individual wants to exercise any of these rights, they should contact the Data Protection Officer. The law does not oblige the Trust to comply with all requests. If the school does not intend to comply with the request then the individual will be notified of the reasons why in writing.

10. Concerns

If an individual has any concerns about how we are using their personal data, we ask that they contact our Data Protection Officer in the first instance. However, an individual can contact the Information Commissioner's Office should they consider this to be necessary, at <https://ico.org.uk/concerns/>.

11. Contact

If you would like to discuss anything in this privacy notice, please contact the Data Protection Office at dpo@fmat.co.uk or by post:

**FAO Data Protection Officer, Fairfax Multi-Academy Trust,
Fairfax Road, Sutton Coldfield,
B75 7JT**

Privacy notice for members/directors/governors

1. Privacy notice for members/directors/governors

Under data protection law, individuals have a right to be informed about how the trust/academy uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals working with the trust as a member/director/associate.

The Trust, Fairfax Multi-Academy Trust is the 'data controller' for the purposes of data protection law, which includes Bournville School, Erdington Academy, Fairfax and Smith's Wood Academy.

2. The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Current and previous contact details – title, name(s), address(es), email address, telephone contact details.
- Date of Birth (D.O.B)
- Current governance positions (type of role appointed to, any positions held on an academy board and term of office).
- Previous governance positions (type of role appointed to, any positions held on an academy board, terms of office served and reasons for resignations/suspensions).
- Training records (of attendance at organised/commissioned training events).
- Attendance at meetings
- Information relating to skills audits undertaken by the Trust
- Signed Code of Conduct, Declaration of Eligibility and Register of Pecuniary Interest forms.
- Information provided by individuals as part of an application form to facilitate the appointment procedure including any references that may be taken.

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This may include information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

3. Why we use this data

The purpose of processing this data is to help us run the trust/academy to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing governors'/directors' details
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Undertake equalities monitoring
- Ensure that appropriate access arrangements can be provided for volunteers who require them

4. Our legal basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation
- Carry out a task in the public interest
- Less commonly, we may also use personal information about you where:
- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify our use of your data.

5. Collecting this information

The information we collect about members/directors/governors is provided by yourself to either the Trust directly or to an academy in our Trust.

6. How we store this data

Personal data is stored in line with our data protection policy.

We maintain a file to store personal information about all volunteers. The information contained in this file is kept secure and is only used for purposes directly relevant to your work with the trust/academy.

When your relationship with the trust/academy has ended, we will retain and dispose of your personal information in accordance with our data protection policy.

7. Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Academies within the Trust where appropriate
- The Department for Education (DfE)
- Other appropriate regulators, such as Ofsted, Regional Schools Commissioners
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as governor/director support and training
- Our legal support professional advisers and consultants

8. Your rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the:

- Right to Access
- Right to Rectification
- Right to Erasure
- Right to Restriction
- Right to Data Portability
- Right to Object
- Right to Complain

If you have any queries regarding any of the above information we hold, please contact the Data Protection Officer whose contact details are recorded below.

9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer (DPO). Alternatively,

you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

10. Contact us

If you would like to discuss anything in this privacy notice, please contact the Data Protection Office at dpo@fmat.co.uk or by post:

**FAO Data Protection Officer, Fairfax Multi-Academy Trust,
Fairfax Road, Sutton Coldfield,
B75 7JT**

Privacy notice for alumni

1. Privacy notice for alumni

Under data protection law, individuals have a right to be informed about how the trust/academy uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals who are former students, which we classify as alumni.

The Trust, Fairfax Multi-Academy Trust is the 'data controller' for the purposes of data protection law, which includes Bournville School, Erdington Academy, Fairfax and Smith's Wood Academy.

2. What personal data do we process?

We may collect, hold, share or otherwise use the following information about you as alumni:

- Full name and former name (if applicable)
- Contact details (email, phone number, address)
- Date of birth
- Years attended and school name
- Current employment and education details (if provided)
- Photographs or stories you choose to share

3. Why we use this data

We may process the data for the following purposes:

- To invite you to reunions, conferences, networking events and/or volunteering opportunities
- To promote the Trust and its academies through alumni stories and testimonials
- For fundraising and development activities (where applicable)
- To maintain accurate alumni records

4. Our legal basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Consent – where you have actively opted in (e.g. to receive communications)
- Legitimate interests - where we have a legitimate interest in staying connected with former students and you would reasonably expect us to do so

You can withdraw your consent or object to processing at any time.

5. Collecting this information

The information we collect about alumni is provided by yourself to either the Trust directly or to an academy in our Trust.

6. How we store this data

Personal data is stored in line with our data protection policy.

We maintain a file to store personal information about alumni. The information contained in

this file is kept secure and is only held for as long as necessary for the purposes it was collected.

When your relationship with the trust/academy has ended, we will retain and dispose of your personal information in accordance with our data protection policy.

7. Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Academies within the Trust where appropriate
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as governor/director support and training
- Our legal support professional advisers and consultants

8. Your rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the:

- Right to Access
- Right to Rectification
- Right to Erasure
- Right to Restriction
- Right to Data Portability
- Right to Object
- Right to Complain

If you have any queries regarding any of the above information we hold, please contact the Data Protection Officer whose contact details are recorded below.

9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer (DPO). Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

10. Contact us

If you would like to discuss anything in this privacy notice, please contact the Data Protection Office at dpo@fmat.co.uk or by post:

**FAO Data Protection Officer, Fairfax Multi-Academy Trust,
Fairfax Road, Sutton Coldfield,
B75 7JT**

Protection of Biometric Information Policy

1. Policy statement

- 1.1. This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:
 - Protection of Freedoms Act 2012
 - Data Protection Act 2018
 - UK General Data Protection Regulation (UK GDPR)
 - DfE 'Protection of biometric information of children in schools and colleges'
- 1.2. This policy operates in conjunction with the following Trust policy and procedures:
 - Data Protection Policy
 - Data Breach Procedure
 - Data Protection Impact Assessment (DPIA) Procedure
 - Subject Access Request (SAR) Procedure
 - Retention Schedule

2. About this policy

- 2.1. This policy and any other documents referred to in it set out the basis on which we will **process** any **biometric information** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.
- 2.2. This policy does not form part of any employee's contract of employment and may be amended at any time.
- 2.3. This policy sets out rules on protecting **biometric information** and the legal conditions that must be satisfied when we process **biometric information**.

3. Definition of biometrics information terms

- 3.1. **Automated biometric recognition system:** A system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with **biometric information** stored in the system to see if there is a match in order to recognise or identify the individual.
- 3.2. **Biometric information:** Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.
- 3.3. **Consent:** **GDPR** requires that **consent** must be freely given, that the academy must keep a record to demonstrate consent; be able to display prominence and clarity of consent requests; and advise the right to withdraw consent easily and at any time.
- 3.4. **Data controller:** Under data protection law, the Trust is the **data controller** for all **biometric information** held by the academies.
- 3.5. **Processing biometric information:** **Processing biometric information** includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:
 - Recording students' **biometric information**, e.g. taking measurements from a fingerprint via a fingerprint scanner.

- Storing students' **biometric information** on a database.
- Using students' **biometric information** as part of an electronic process,
- e.g. by comparing it with **biometric information** stored on a database to identify or recognise students.

3.6. **Special category data: Personal data** which the **GDPR** says is more sensitive, and so needs more protection – where **biometric information** is used for identification purposes, it is considered **special category data**.

4. Roles and responsibilities

- 4.1. The Trust's **Audit & Risk Committee (ARC)** are responsible for approving this policy.
- 4.2. **Academy Principals** are responsible for ensuring the provisions in this policy are implemented consistently.
- 4.3. The Trust's **Data Protection Officer (DPO)** is responsible for;
- Monitoring the academy's compliance with data protection legislation in relation to the use of **biometric information**.
 - Advising on when it is necessary to undertake a **data protection impact assessment (DPIA)** in relation to the academy's biometric system(s).
 - Being the first point of contact for the **Information Commissioners Office (ICO)**.

5. Data protection principles

- 5.1. The academy processes all **personal data**, including **biometric information**, in accordance with the key principles set out in the **GDPR**.
- 5.2. The academy must ensure **biometric information** is:
- Processed lawfully, fairly and in a transparent manner.
 - Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
 - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
 - Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
 - 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.
 - Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 5.3. The Trust is **data controller**, the academy is responsible for being able to demonstrate its compliance with the provisions outlined in 5.2.

6. Data protection impact assessments (DPIAs)

- 6.1. Prior to processing biometric information or implementing a system that involves processing biometric information, a **DPIA** will be carried out.
- 6.2. The **DPO controls** the **Data Protection Impact Assessment (DPIA)** procedure for the Trust and must be contracted prior to beginning a **DPIA**.
- 6.3. The **DPO** will oversee and monitor the process of carrying out the **DPIA**, the **DPIA** will:
- Describe the nature, scope, context and purposes of the processing.

- Assess necessity, proportionality and compliance measures.
 - Identify and assess risks to individuals.
 - Identify any additional measures to mitigate those risks.
- 6.4. When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.
- 6.5. If a high risk is identified that cannot be mitigated, the **DPO** will consult the **ICO** before the processing of the **biometric information** begins.
- 6.6. The **ICO** will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In some cases, the **ICO** may advise the school to not carry out the processing.
- 6.7. The Trust will adhere to any advice from the **ICO**.

7. Consent

- 7.1. Prior to any **biometric recognition system** being put in place or processing of **biometric information**, the academy must request written **consent** for the use of **biometric information**.
- 7.2. **Consent** must be freely given. Academies must request written consent advising an explicit yes or no answer to consenting to the processing of **biometric information**.
- 7.3. **Consent** must not be gained through an opt-out option.
- 7.4. If there is no reply to the **consent** request, the academy must determine this as **consent** is not provided.
- 7.5. The academy must keep a record of **consent** as part of the student/staff file.
- 7.6. Request for **consent** from individuals must advise the following:
- Details about the type of **biometric information** to be taken
 - Details of the system(s) that will be used to hold and process the **biometric information**
 - How the **biometric information** will be used
 - The right to refuse or withdraw their consent
 - The academy's duty to provide reasonable alternative arrangements for those students whose information cannot be processed
- 7.7. Consent can be withdrawn at any time, see 8.9 for withdrawal of student biometric information, and 9.2 for staff withdrawal.
- 7.8. Alternative arrangements must be provided to any individual that does not **consent** to take part in the academy's **biometric system(s)**, in line with section 10 of this policy.

8. Student Consent

- 8.1. **Consent** for the processing of **biometric information** of children under the age of 18 is not imposed by the **Data Protection Act 2018** or the **GDPR**. Instead, the consent requirements for biometric information is imposed by **section 26** of the **Protection of Freedoms Act 2012**.
- 8.2. In line with both the **Protection of Freedoms Act 2012** and **GDPR** for students' in Year 9 or above, the academy will request **consent** from the student as well as the parent. See **Appendix 1** for an overview of the requirements.

- 8.3. The written **consent** of at least one parent must be obtained before the data is taken from the student and used. This applies to all students under the age of 18. In no circumstances can a student's **biometric information** be processed without written consent from parents.
- 8.4. The written **consent** of students in Year 09 or above must also be obtained before the data is taken from the student and used. For students already on roll, the written **consent** of students must be sought during the Autumn Term of Year 09.
- 8.5. Academies must ensure that each parent of a child is notified of the academy's intention to use a student's **biometric information** as part of an **automated biometric recognition system**.
- 8.6. Where the name of only one parent is included on the admissions register, the academy will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.
- 8.7. The academy does not need to notify a particular parent or seek their **consent** if it is satisfied that:
- The parent cannot be found, e.g. their whereabouts or identity is not known.
 - The parent lacks the mental capacity to object or **consent**.
 - The welfare of the student requires that a particular parent is not contacted, e.g. where a student has been separated from an abusive parent who must not be informed of the student's whereabouts.
 - It is otherwise not reasonably practicable for a particular parent to be notified or for their **consent** to be obtained.
- 8.8. Where neither parent of a student can be notified for any of the reasons set out in 8.6, **consent** will be sought from the following individuals or agencies as appropriate:
- If a student is being 'looked after' by the **Local Authority (LA)** or is accommodated or maintained by a voluntary organisation, the **LA** or voluntary organisation will be notified, and their written consent obtained.
 - If the above does not apply, then notification will be sent to all those caring for the student and written consent will be obtained from at least one carer before the student's biometric information can be processed.
- 8.9. The academy will not process the **biometric information** of a student under the age of 18 in the following circumstances:
- The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric information
 - No parent or carer has consented in writing to the processing.
 - A parent or carer of the student has objected in writing to such processing, even if another parent has given written consent.
- 8.10. Parents and students can object to participation in the academy's biometric system(s) or withdraw their consent at any time. Where this happens, any **biometric information** relating to the student that has already been captured must be deleted.
- 8.11. If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their **biometric information**, the academy will ensure that the student's **biometric information** is not taken or used as part of a **biometric recognition system**, irrespective of any consent given by the student's parent(s).
- 8.12. **Consent** is considered valid for the duration of a student's for the duration that the student is on roll at the academy unless **consent** is withdrawn by the student or parent.

9. Staff consent

- 9.1. Where staff members or other adults use the academy's **biometric system(s)**, **consent** will be obtained from them before they use the system.
- 9.2. Staff and other adults can object to taking part in the **academy's biometric system(s)** and can withdraw their **consent** at any time. This must be in writing. Where this happens, any **biometric information** relating to the individual that has already been captured must be deleted.
- 9.3. For staff, **consent** is considered valid for the duration of employment, unless **consent** is withdrawn.

10. Alternative arrangements

- 10.1. Parents, students, staff members and other relevant adults have the right to not take part in the **academy's biometric system(s)**.
- 10.2. Where an individual objects to taking part in the academy's **biometric system(s)**, reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a **biometric system** uses student's fingerprints to pay for school meals, the student will be able to use a pre-programmed card, unique number or other suitable means determined by the academy.
- 10.3. Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the student's parents, where relevant).

11. Data Retention

- 11.1. **Biometric information** will be managed and retained in line with the Trust's **retention schedule**.
- 11.2. If an individual (or a student's parent, where relevant) withdraws their **consent** for their/their child's **biometric information** to be processed, it must be erased from the academy's system(s) without undue delay.

12. Data Breaches

- 12.1. The Academy is responsible for ensuring there are appropriate and robust security measures in place to protect the **biometric information** held by the academy.
- 12.2. Any suspected data breach must be immediately reported to the **Academy Principal** and the Trust's **Data Protection Officer (DPO)**.
- 12.3. Any suspected data breach to the academy's biometric system(s) will be dealt with in accordance with the Trust's **Data Protection Policy** and be reviewed using the Trust's **Data Breach Procedure**.

13. Subject access requests (SAR)

- 13.1. Any subject access requests (SAR) for biometric information will be dealt with in accordance with the Trust's **Data Protection Policy** and be reviewed using the Trust's **Subject Access Request (SAR) Procedure**.

14. Monitoring and review

- 14.1. The **Trust Data Protection Officer** is responsible for reviewing this document annually.

APPENDIX 1 - OVERVIEW OF STUDENT CONSENT COLLECTION



NEW STUDENTS JOINING THE ACADEMY

New Student Joining the Academy	Reception Year 01 Year 02 Year 03 Year 04 Year 05 Year 06							Year 07 Year 08 Year 09 Year 10 Year 11					Year 12 Year 13	
	Notify both parents of biometric consent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Written consent from one parent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Written consent from students	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes

EXISTING STUDENTS ON ROLL AT THE ACADEMY

Existing Students at the Academy	Reception Year 01 Year 02 Year 03 Year 04 Year 05 Year 06							Year 07 Year 08 Year 09 Year 10 Year 11					Year 12 Year 13	
	Notify both parents of biometric consent	NOTIFY PARENTS PRIOR TO STUDENT JOINING THE ACADEMY												
Written consent from one parent	COLLECT CONSENT PRIOR TO STUDENT STARTING ACADEMY – LASTS DURATION OF STUDENT BEING ON ROLL													
Written consent from students										COLLECT IN Y9 – LASTS DURATION				