



FRMAT DATA PROTECTION POLICY

Updated: May 2025

Updated May 2026: Privacy Notices (Appendices 1 and 2) updated; Appendix 4 (APD) added

Trustee approval date: May 2026

Introduction

- 2.1) The Five Rivers Multi Academy Trust and the academies within it collect and use personal data and information about staff, pupils, parents and other individuals who come into contact with the Trust/ academies. This data/information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use data/information to ensure that the Trust/academies comply with their statutory obligations.
- 2.2) Academies/Trusts have a duty to be registered as Data Controllers with the Information Commissioner's Office (ICO), detailing the data/information held and its use. These details are then available on the ICO's website. Academies also have a duty to issue a Fair Processing Notice/Privacy Notice to all pupils/parents. This summarises the data and information held on pupils, why it is held and the other parties to whom it may be passed on.
- 2.3) The policy refers to all data collected and all information derived from the data.

Purpose

- 2.4) This policy is intended to ensure that personal data and information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulation (UK GDPR), and the [Data Protection Act 2018 \(DPA 2018\)](#). It will apply to data/information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.
- 2.5) All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

- 2.6) Personal information is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

- 2.7) The UK GDPR establishes eight enforceable principles that must be adhered to at all times:
 - 1. Personal data shall be processed fairly and lawfully and in a transparent manner in relation to individuals;
 - 2. Personal data shall be obtained only for one or more specified, explicit and lawful purposes and not further processed in a manner that is incompatible with those purposes;
 - 3. Personal data shall be adequate, relevant and not excessive, limited to what is necessary in relation to the purposes for which it is processed;
 - 4. Personal data shall be accurate and where necessary, kept up to date;
 - 5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;

6. Personal data shall be processed in accordance with the rights of data subjects under the UK GDPR;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Accountability and governance is a significant addition to the legislation under the UK GDPR: the data controller 'shall be responsible for, and be able to demonstrate, compliance with the principles'.

General Statement

- 2.8) The Trust and its academies are committed to maintaining the above principles at all times.

Therefore the Trust and its academies will:

- Inform individuals why the data/information is being collected when it is collected. This will take the form of Privacy Notices (one for staff and one for pupils / parents) which are to be displayed on the academy (and Trust) website – these are contained within this toolkit at the end of Section Two.
- Ensure that verifiable consent is given from individuals for their data to be processed (this must be opt-in – silence, pre-ticked boxes or inactivity do not constitute consent). A record must be kept of how and when consent was given. Individuals have a right to withdraw consent at any time.
- Inform individuals when their data or information is shared, and why and with whom it was shared;
- Check the quality and the accuracy of the data/information it holds. Individuals have a right to rectification of personal data if it is inaccurate or incomplete. If the data has already been disclosed to a third party, they must also be advised of the rectification where possible;
- Ensure that data/information is not retained for longer than is necessary;
- Ensure that when obsolete data/information is destroyed that it is done so appropriately and securely;
- Ensure that clear and robust safeguards are in place to protect personal data / information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Share data/information with others only when it is legally appropriate to do so;
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal data/information, known as Subject Access Requests (section 5);
- Ensure our staff are aware of and understand our policies and procedures.
- Maintain minimum standards for creation of paper or electronic records and establish procedures to ensure that there is a legitimate purpose for using personal data prior to collecting it.
- Establish procedures and guidelines for staff to ensure new records are titled and indexed in a way that allows efficient management, retrieval and disposal.

Outsourcing

- 2.9) Should any personal data be outsourced for processing, the Trust will ensure that a contractor is chosen which provides sufficient guarantees about how it will protect the data, and will ensure that written and enforceable contracts are in place setting out information security conditions. Consideration will also be given to whether outsourcing involves the transfer of data overseas, and if so the Trust will ensure that the recipient will provide adequate protection.

Privacy Impact Assessments

- 2.10) The Trust will build in privacy considerations at the start of all new projects or initiatives that involve the processing of personal data. Privacy impact assessments will be undertaken during the development, testing and delivery stages, and supporting guidelines for staff will be implemented.
- 2.10.1) Principals are responsible for ensuring that Privacy Impact Assessments are carried out during the development, testing and delivery stages of any new academy level project.
- 2.10.2) The PA to the CEO/DBS is responsible for ensuring that Privacy Impact Assessments are carried during the development, testing and delivery stages of any new trust wide or trustee level project.
- 2.10.3) The template for the Privacy Impact Assessment is at the end of this section.

The Impact of AI on Data Protection

While not a legislative change, there has recently been significant focus on how AI tools interact with data protection requirements.

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Microsoft Co-pilot and Google Gemini. We recognise that AI has many uses, but also poses risks to sensitive and personal data. FRMAT is committed to ensuring that all AI use complies with the Data Protection Act 2018 and UK GDPR. We understand that AI tools can process, store, and in some cases train models on the data provided to them, which presents specific data protection risks.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter any personal or identifiable information into unauthorised generative AI tools or chatbots. This includes pupils' names, staff details, sensitive safeguarding information, special category data, or any other information that could identify an individual.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, FRMAT will treat this as a data breach, and will follow the personal data breach procedure outlined in Appendix 4.

Should FRMAT approve the use of a 'closed' AI tool which is designed for institutional use and complies with our data protection requirements, we will ensure that appropriate safeguards are in place, including data processing agreements with suppliers and updated privacy notices to inform everyone concerned about how their data is being used.

Before introducing any new AI tool or using an existing tool in a new way, we will conduct a Data Protection Impact Assessment (DPIA) to identify and mitigate risks. Our Data Protection Officer will be consulted throughout this process and will provide guidance to staff on the safe and compliant use of AI tools. We will maintain a whitelist of approved AI tools that have been risk-assessed and are safe for use with school data (please see the whitelist in the appendix of the **FRMAT AI Policy**).

All staff receive regular training on data protection, including specific guidance on AI use. We monitor developments in AI technology and regularly review our approach to ensure we continue to meet our data protection obligations whilst making effective use of technology to support teaching, learning, and school operations. Any concerns about AI use and data protection should be reported immediately to the Data Protection Officer (Andy Wynne andy.wynne@learnsheffield.co.uk)

Further details about our approach to AI can be found in the **FRMAT AI Policy** and the **Staff ICT Acceptable Use Policy**.

Complaints

2.11) Complaints will be dealt with in accordance with the Trust's / academy's complaints policy. Complaints relating to data/information handling may be referred to the Information Commissioner (the statutory regulator).

Appendices:

Appendix 1: Privacy Notice for Parents and Pupils

(Principals are responsible for ensuring this is displayed on the academy website and handed to new parents upon induction)

Appendix 2: Privacy Notice for Staff (Principals are responsible for ensuring this is disseminated to all staff members including new staff at the point of induction)

Appendix 3: Privacy Impact Assessment Guidance and Templates (The Director of Business Strategy and Principals are responsible for completing these during the development, testing and delivery stages of any new project)

Appendix 4: Appropriate policy Document

Appendix 1: Privacy Notice for parents and carers and their children's data

1. Introduction

Under UK data protection law, individuals have a right to be informed about how our school 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 **pupils at our school and their parents/carers**.

We, FRMAT and its academies, are the 'data controllers' for the purposes of UK data protection law.

Our data protection officer is **Andy Wynne** (see 'Contact us' below).

2. The personal data we hold

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

- Contact details and contact preferences (such as your names, address, email address and telephone numbers),
- Pupil date of birth, identification documents
- Parents/carers email addresses, telephone numbers
- Details of your family circumstances
- Records of your correspondence and contact with us
- Details of any complaints you have made
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Attendance information
- Details of any safeguarding information including court orders or professional involvement
- Details of any support received, including care packages, plans and support providers
- Photographs, videos and CCTV images captured in school
- Data about use of the school's information and communications systems, equipment and facilities (e.g. school computers)

We may also collect, use, store and share (when appropriate) information about you or your child that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to:

- Information about any medical conditions we need to be aware of, including physical and mental health
- Information about characteristics, such as ethnicity, [religion], languages spoken or special educational needs

We may also hold data about your child that we have received from other organisations, including other schools and social services.

3. Why we use this data

We use the data listed above to:

- Support pupil learning
- Monitor and report on pupil attainment and progress
- To contact you about your child and the running of the school
- Provide appropriate pastoral care
- Protect pupil welfare and keep children safe (e.g. food allergies, or emergency contact details)
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing
- Meet the statutory duties placed upon us for the Department for Education data collections
- Keep you informed about the running of the school (such as emergency closures) and events
- Process payments for school services and clubs
- Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

3.1 Use of your child's personal data in automated decision making and profiling

We do not currently process any pupils' personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

3.2 Use of your child's personal data for filtering and monitoring purposes

While your child is in our school, we may monitor their use of our information and communication systems, equipment and facilities (e.g. school computers). We do this so that we can:

- Comply with health and safety and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use policy) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- Protect your child's welfare

4. Our lawful basis for using this data

Our lawful basis for processing you and your child's personal data for the purposes listed in section 3 above are as follows:

- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations). We need to process data to meet our responsibilities as a school under UK law as set out here: <https://www.gov.uk/government/collections/statutory-guidance-schools> An example of this is 'safeguarding children and young people'

- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. Managing a school is considered a '**task in the public interest**'. Further details are available here: <https://www.gov.uk/government/collections/statutory-guidance-schools>

Less commonly, we may also use personal information about you where:

- We ask for your **Consent:** the individual has given clear consent for you to process their (or their child's) personal data for a specific purpose. An example of this may be certain uses of photographs of your child.
- We need to protect an individual's **vital interests** (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- 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.

Where you have provided us with consent to use your data or your child's data, you may withdraw this consent at any time. We will make this clear when requesting consent, and explain how you would 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 the school's use of your data.

4.1 Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your child's personal data in a certain way
- We need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- We need to process it for the establishment, exercise or defence of legal claims
- We need to use it for reasons of substantial public interest as defined in legislation
- We need to process it 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
- We need to use it for public health reasons, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public interest

5. Collecting this data

While the majority of information we collect about you and your child is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about your child will come from you, but we may also hold data about your child from:

- Sheffield City Council
- A previous school
- Government departments or agencies
- Health authorities or GP practices
- Police forces, courts or tribunals
- Use of the school network and equipment via our appropriate filtering and monitoring systems in line with [DfE guidance](#) and KCSIE2023

6. How we store this data

We keep personal information about you and your child while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary. Our record retention policy sets out how long we keep information about pupils.

If you wish to see a copy of the schools retention policy please ask at the main school office.

We have put in place appropriate security measures to prevent you and your child's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of personal data pertaining to you and your child securely when we no longer need it.

7. Who we share data with

We routinely share pupil information with:

- Schools that the pupils attend after leaving us
- Our local authority Sheffield City Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions
- The Department of Education for statutory data collections such as the school census

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

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

- The pupil's family and representatives
- Our regulator, Ofsted
- Exam boards
- Suppliers and service providers:
- Learn Sheffield – a School Company of which this school is a member
- Specific types of providers (e.g. catering, IT provider, filtering and monitoring providers)
- Financial organisations
- Our auditors
- Survey and research organisations
- Local Health authorities
- Security organisations
 - Health and social welfare organisations
 - Professional advisers and consultants
- Charities and voluntary organisations

- Police forces, courts, tribunals

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census and early years census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with third parties, such as other organisations which promote children's education or wellbeing in England. These third parties must agree to strict terms and conditions about how they will use the data. For more information, see the Department's webpage on how it collects and shares personal data.

You can also contact the Department for Education with any further questions about the NPD.

8. Your rights

8.1 How to access personal information that we hold about you and your child

You have a right to make a 'subject access request' to gain access to personal information that we hold about you and your child.

If you make a subject access request, and if we do hold information about you and your child, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your child's personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

8.2 Your right to access your child's educational record

Parents, or those with parental responsibility, also have the right to access their child's educational record (which includes most information about a pupil). This right applies as long as the pupil is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced. To make a request, please contact the main school office.

8.3 Your other rights regarding you and your child's data

Under UK data protection law, you have certain rights regarding how you and your child's personal data is used and kept safe. For example, you have the right to:

- Object to our use of you and your child's personal data
- Prevent you and your child's data being used to send direct marketing
- Object to and challenge the use of you and your child's personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected
- In certain circumstances, have the personal data we hold about you and your child deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided consent for your personal information to be collected, processed and transferred for a particular reason
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' 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.

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

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

10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

FRMAT Central Team:

Emma Farmer (Director of Business Strategy) efarmer@fiveriversmat.uk

Tinsley Meadows:

Tania Macpherson (Principal) tmacpherson@tinsleymeadows.sheffield.sch.uk

Abbeyfield:

Kate Abell (Principal) kabell@abbeyfield.sheffield.sch.uk

Or

FRMAT Data Protection Officer: Andy Wynne andy.wynne@learnsheffield.co.uk

Reviewed May 2026 AB

Appendix 2: Privacy Notice for staff of Five Rivers Multi Academy Trust

1. Introduction

Under UK data protection law, individuals have a right to be informed about how our school / trust (delete as applicable) 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 we employ, or who otherwise engage with our school** in roles such as volunteers, governors/trustees.

We, FRMAT and its academies, are the 'data controllers' for the purposes of UK data protection law.

Our data protection officer is **Andy Wynne** of **Learn Sheffield** (see 'Contact us' below).

2. The personal data we hold

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

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information [Paid roles only]
- Bank account details, payroll records, National Insurance number and tax status information [paid roles only]
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- (For governors/trustees) Governance details (such as role, start and end dates and governor ID)
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence or other evidence of identity
- (For governors/trustees) Information about business and pecuniary interests
- Photographs and CCTV images captured in school/on site
- Data about your use of the school's information and communications system, equipment and facilities
- Results from online searches during the recruitment process

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to:

- Information about any health conditions you have that we need to be aware of including information about disability and access requirements

- Absence & Sickness records, occupational health referrals and reports or statements of fitness for work from you GP or hospital
- Ethnicity

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service (DBS) in respect of criminal offence data.

3. Why we use this data

We use the data listed above to:

- a Enable you to be paid [where applicable]
- b Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- c Support effective performance management
- d Inform our recruitment and retention policies
- e Allow better financial modelling and planning
- f Enable equalities monitoring
- g Improve the management of workforce data across the sector
- h Ensure that appropriate access arrangements can be provided for people that require them
- i Establish and maintain effective governance
- j Meet statutory obligations for publishing and sharing details about employees, trustees and governors
- k Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely
- l To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- m Support the work of the School Teachers' Review Body

3.1 Use of your personal data in automated decision making and profiling

We do not currently process any staff members personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

3.2 Use of your personal data for filtering and monitoring purposes

While you're in our school, we may monitor your use of our information and communication systems, equipment and facilities (e.g. school computers). We do this so that we can:

- Comply with health and safety and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use policy) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)

4. Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed in section 3 above are as follows:

- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. For example: Employed staff have a contract with the school/trust
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations). We need to process data to meet our responsibilities under law as set out here: <https://www.gov.uk/government/collections/statutory-guidance-schools> An example of this is 'safeguarding children and young people'
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. Managing a school is considered a 'task in the public interest'. Further details are available here: <https://www.gov.uk/government/collections/statutory-guidance-schools>
- Ask for your **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. An example of this may be certain uses of photos of you.

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 would 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 the school's use of your data.

4.1 Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it 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
- We need to process it 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
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your **consent** to use it in a specific way
- We need to protect an individual's **vital interests** (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been **made manifestly public** by you
- We need to process it for, or in connection with, **legal proceedings**, to obtain legal advice, or for the establishment, exercise or defence of legal rights

- We need to process it for reasons of **substantial public interest** as defined in legislation

5. Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- Local authorities
- Health Authorities, GPs or Occupational Health
- Government departments or agencies
- Police forces, courts or tribunals
- Previous employer or Personal Referee
- Your use of the school network and equipment via our appropriate filtering and monitoring systems in line with [DfE guidance](#)
- Online searches carried out by the [school/trust] or on behalf of the [school/trust] in-line with the DfE [KCSIE 2023 guidance](#) Section 221. *“...as part of the shortlisting process schools and colleges should consider carrying out an online search as part of their due diligence on the shortlisted candidates.”*

6. How we store this data

We keep personal information about you while you work at our trust. We may also keep it beyond your employment at our school if this is necessary. Our data retention policy sets out how long we keep information about staff. For a copy of this please contact the school office.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

7. Who we share data with

We routinely share information with:

- Our local authority, Sheffield City Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Learn Sheffield Governance Service
- The Department of Education - e.g. workforce census, Get Information About Schools (GIAS) or in line with statutory requirements for specific governance roles, e.g. PRUs

We do not share information about you with any third party without consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with UK data protection law), we may also share personal information about you with:

- Your family and representatives - next of kin in an emergency
- Ofsted, our regulator
- Suppliers and service providers:
 - Specific types of providers (e.g. catering, HR)
 - Employment checking services e.g. DBS
- Financial organisations such as South Yorkshire Pension Authority – LGPS
- Future employers for references
- Our auditors
- Survey and research organisations e.g. School Teachers' Review Body
- NHS teams and professionals
- Health and social welfare organisations
- Police forces, courts or tribunals - only when required by law
- Professional advisers and consultants
- Charities and voluntary organisations
- Employment and recruitment agencies - e.g. references

8. Your rights

8.1 How to access personal information that we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

8.2 Your other rights regarding your data

Under UK data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- Object to our use of your personal data
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected
- In certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose

- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact us (see 'Contact us' 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.

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

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

10. Contact us

If you want to see a copy of the information about you that we hold, or if you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

- FRMAT Central Team: Emma Farmer (Director of Business Strategy) efarmer@fiveriversmat.uk
- Tinsley Meadows: Tania Macpherson (Principal) tmacpherson@tinsleymeadows.sheffield.sch.uk
- Abbeyfield: Kate Abell (Principal) kabell@abbeyfield.sheffield.sch.uk

Or

- FRMAT Data Protection Officer: Andy Wynne andy.wynne@learnsheffield.co.uk

Appendix 3a: Privacy Impact Assessments - Guidance

Definition of Privacy

Privacy, broadly speaking, is the right to be left alone, or freedom from interference or intrusion. Examples of types of privacy are as follows:

- a) data or information privacy – these are rights covered by the UK GDPR. Individuals have rights in relation to the personal data which is held and processed about them by organisations.
- b) privacy of the person in particular, for example having the right to privacy in a toilet cubicle or other private space.
- c) privacy of personal behaviour, for example where surveillance (CCTV, for instance) or monitoring is involved.
- d) privacy in communications, for example bugging of telephones and monitoring of telephones and emails.

The Human Rights Act guarantees a right to respect for private life which can only be interfered with when it is necessary to meet a legitimate social need.

Introduction

Loss of privacy is a risk, so a Privacy Impact Assessment (PIA) should be built into project management processes and risk management processes. It enables problems to be dealt with at an early stage, by identifying and minimising privacy risks.

Benefits of conducting a PIA include:

- reassurance for the individual and the organisation
- procedures are simplified
- the organisation collects less data
- costs are lowered
- awareness of privacy and data protection issues are raised.

Step 1 – Identify the need for a PIA

A PIA should be considered for any of the following:

- New projects / plans / proposals
- New administrative systems with privacy implications
- Outsourcing a system
- New technology/ new methods of electronic communications
- New IT systems
- Sharing of personal data with other bodies
- Surveys
- New or different use of personal data
- New policies, or statutory duties
- Whenever there is a potential for damage or distress to individuals.

Any member of staff who is considering one of the above should initially answer these screening questions:

	Yes	No
1. Will the project involve the collection of new information about individuals?		
2. Will the project compel individuals to provide information about themselves?		
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
4. Will the information about individuals be used for a purpose for which it is not currently used, or in a way it is not currently used?		
5. Would the individuals concerned have a reasonable expectation that the information about them wouldn't be used in this way? i.e. it would be an unexpected use.		
6. Does the project involve new technology which might be perceived as being privacy intrusive?		
7. Will the project result in decisions or action being taken against individuals in ways which can have a significant impact on them?		
8. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, is it sensitive personal information, or information that people would consider to be particularly private?		
9. It is not possible or feasible for individuals to opt out of the system.		
10. It is not possible or feasible to ask individuals to give consent to the system.		
11. Will the project require individuals to be contacted in ways which they may find intrusive?		
12. The impact on privacy may be disproportionate to the outcomes which will be achieved by the project. Is this the case?		

If the answer to **any** of these is Yes, then the PIA should be conducted – go to the FRMAT template PIA form and fill it in, using the guidance following here.

Step 2 - Describe information flows or procedures

A full understanding of how information will be used is needed. Consider the following:

- Has the **purpose** of the project / process been identified? What is it intending to achieve?
- How will information be **obtained**, **used** and **retained**? It is important at this early stage to identify all of the purposes for which the information might be used in the future.
- If **new software** is being procured does it allow the amending, deleting and archiving of data when necessary?

- If the project involves **marketing**, is there a procedure for individuals to opt out of their information being used for that purpose?
- How will the **accuracy** of the personal data to be obtained from individuals or other organisations be ensured?
- If **transfers** of data will be made to other people or bodies, how will the data be adequately **protected**?
- Will the project require data to be transferred **outside of the EEA**? (This includes potentially placing data on the **internet** or in the **cloud**.) If so, how will this be managed?
- **How many** individuals will be affected?
- How will individuals be **told** about the use of their personal data?
- What are those individuals' **reasonable expectations** with regards to the data?
- Does the Trust need to amend its **privacy notices**?
- If **consent** is being relied on to process personal data, how will this be collected and what will happen if it is withheld or withdrawn?

Step 3 - Identify the privacy risks

Consider what are the risks to individuals and the Trust. The more intrusion into a person's privacy there is, the higher is the risk of impact, or risk of harm.

Risk arises through personal information being:

- inaccurate, insufficient or out of date
- excessive or irrelevant
- kept for too long
- disclosed to those who the person it is about does not want to have it
- used in ways that are unacceptable to or unexpected by the person it is about
- not kept securely
- transferred outside the European Economic Area or placed on the internet or in the cloud.

Harms for individuals could include:

- financial loss
- losing a job
- risks to physical safety
- damage to personal relationships and social standing
- identity theft
- loss of personal autonomy or dignity
- excessive surveillance
- legal action
- distress, including fear of all of the above.

Harms for the organisation include:

- financial damage
- risk of fines, or other legal action
- reputational damage
- loss of business
- failure of the project or deterioration or changes to the aims of the project.

Step 4 – Solutions to the identified risks

Changes to the project / process should be considered at this stage, in order to devise ways to reduce the risks. It is possible that the conclusion will be reached that some risks are necessary. It might be that some risks are not acceptable, and will need to be eliminated. In order to decide whether risks need to be eliminated, or reduced, or accepted, the project outcomes need to be balanced against the impact on individuals. Consider the following:

- Is it **necessary** to collect or process all the pieces of information originally included in the plan, without compromising the needs of the project?
- Think about the **retention period** of the data and how it will be destroyed.
- Think what **security measures** will be put in place. Does the new system provide adequate protection against security risks?
- **Train staff** where necessary so that they can operate the new system or manage the new process satisfactorily and securely.
- **Anonymise** data where possible.
- Provide **guidance** for staff where necessary.
- Make data subjects **aware** of the data collection.
- If the project involves marketing, include a procedure for individuals to **opt out** of their information being used for that purpose.
- Make sure that **agreements / contracts** are in place with external data controllers or processors. This includes data sharing agreements where applicable.
- Is an update of the Trust's entry in the **register of data controllers** necessary (where new purposes for processing personal data have been identified)? Contact the Trust's Chief Operating Officer (the CEO) for advice.

Steps 2 - 4 – During all of these steps, consult with internal and external stakeholders as needed throughout the process

These people could include:

- The project team
- The Trust's Information Lead (Director of Business Strategy)
- Staff with a responsibility for risk management
- The designers of the project / system
- IT staff
- Procurement staff
- Staff with a responsibility for communications
- Users of the system, both internal and external
- Senior management

Step 5 - Sign off and record

The PIA should be signed off by the relevant person, and integrated into the project plan. If the risk is not high, the relevant Project Manager may sign off. A Privacy Impact team made up of the Information Officer, the Risk Manager, and the Chief Operating Officer should sign off projects of medium or high risk. The PIA should be kept as a record, and a log of Assessments will be kept by the Chief Operating Officer.

Appendix 3b: Privacy Impact Assessment Template

Privacy is the right to be left alone, or freedom from interference or intrusion.

Assessments into the risk of a loss of privacy for individuals should be made by staff in certain circumstances, such as the following:

- New projects / plans / proposals
- New administrative systems with privacy implications
- Outsourcing a system
- New methods of electronic communications
- New IT systems
- Sharing of personal data with other bodies
- Surveys
- New or different use of personal data
- New policies, or statutory duties
- Whenever there is a potential for damage or distress to individuals

Name / brief description of Project: _____

1. Information flows or procedures

1.1 What are the aims of the project / the purposes for collecting the data?
1.2 <i>How will the data / information be obtained, used and retained?</i>
1.2.1 Where is the information coming from?
1.2.2 If new software, can data be amended / deleted / archived if necessary?
1.2.3 If marketing, can individuals opt out? If not, why not?
1.2.4 How will the accuracy of the data be ensured?

1.2.5 How will transfers of data to other people or bodies be managed?
1.2.6 Will the project require data to be transferred outside the EEA? Placed online or in the cloud? If so, how will this be managed?
1.2.7 How many individuals will be affected by the project?
1.2.8 How will individuals be told about the use of their personal data?

2. Privacy risks

	Description of risk	Assessment of likelihood / impact of risk – Low/Medium/High
Risk 1		
Risk 2		
Risk 3		
Risk 4		
Risk 5		

3. Solutions to the identified risks

Consider the following:

- Reduction of data collected
- Retention period
- Destruction of data
- Security measures

- Staff training and guidance on the system
- Anonymisation of data
- Data subject awareness / opt out
- Agreements / contracts in place with external data controllers or processors, including data sharing agreements
- Consult with internal / external stakeholders

	Solution / partial solution to risk
Risk 1	
Risk 2	
Risk 3	
Risk 4	
Risk 5	

Name:

Role:

Date:

Signed off by:

(if necessary please refer to *Privacy Impact Assessment Guidance*)

Date:

Appendix 4: Appropriate Policy Document (APD)

Our processing of special categories of personal data and criminal offence data

As part of our schools functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special category data

Special category data is defined at Article 9 UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation

It is also important to be aware that some of the [nine protected characteristics outlined in the Equality Act 2010](#) are classified as special category data. These include **race**, **religion or belief**, and **sexual orientation**. They may also include **disability**, **pregnancy**, and **gender reassignment** in so far as they may reveal information about a person's **health**.

Criminal conviction data

Article 10 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

This policy document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices which are available on the school/trust website here. [link to privacy notices]

Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR Articles:

1. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the [school/trust] or the data subject in connection with **employment**, social security or social protection.

Examples include our processing of staff sickness absences.

2. Article 9(2)(g) - reasons of **substantial public interest**.

The school/trust is a public body. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.

An example of this processing would include sharing special category data with the DfE when required, for example as part of the school census.

3. Article 9(2)(j) – for **research** purposes in the public interest.

The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – research.

An example of our processing is working with universities and the Department of Education to provide data for research purposes to help improve UK schools and education.

4. Article 9(2)(h) – the treatment or the **management of health**.

Examples include our processing of data received from an NHS professional or other healthcare worker about one of our students.

5. Article 9(2)(i) – for reasons of public interest in the area of **public health**.

Examples include our sharing data about our staff or students with the NHS in the case of a pandemic.

6. Article 9(2)(a) – **explicit consent**

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include information about student or staff dietary requirements, allergies and other health information that we require to look after the wellbeing of our students and workforce.

When we ask for ethnicity (requested by the DfE for school census returns) we make it clear that providing it is optional and by providing it the data subject (or their parent/carer) is consenting for it to be shared with the DfE.

7. Article 9(2)(c) – where processing is necessary to protect the **vital interests** of the data subject or of another natural person.

An example of our processing would be using health information about a student or member of staff in a medical emergency.

We process criminal offence data under Article 10 of the UK GDPR

Examples of our processing of criminal offence data include pre-employment checks (DBS, barred list) and declarations by a member of the school/trust workforce in line with contractual or safeguarding obligations.

Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for the school. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Description of data processed

- Health and medical data - workforce and students
- Ethnicity - students and workforce
- [Religion - students and workforce]
- [Biometric data (facial recognition) on school/trust provided mobile devices]
- [Trade union membership - staff]
- Criminal records - DBS checks for all members of the school workforce (paid and unpaid)

Further information about this processing can be found in our privacy notices.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special category data

We process SC data for the following purposes in Part 1 of Schedule 1:

- **Paragraph 1(1)** employment, social security and social protection.

We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- **Paragraph 6(1) and (2)(a)** Statutory etc and government purposes
- **Paragraph 8(1) and (2)** Equality of opportunity or treatment
- **Paragraph 18(1)** Safeguarding of children and of individuals at risk

Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- **Paragraph 1** – employment, social security and social protection

Procedures for ensuring compliance with the principles

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary to function as a school/trust under the Education Act 2005

Our processing for the purposes of employment relates to our obligations as an employer.

We also process special category personal data to comply with other obligations imposed on the school/trust by the Department for Education or our local authority.

Principle (b): purpose limitation

We process personal data for the purposes explained above when the processing is necessary for us to fulfil our statutory functions as a [school/trust]

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle (e): storage limitation

All special category data processed by us for the purpose of employment or substantial public interest is retained for the periods set out in our retention schedule

We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)

Electronic information is processed within our secure network. Paper copies of personal data are kept locked in filing cabinets in locked offices.

Our electronic systems and physical storage have appropriate access controls applied, only relevant staff have access to the files.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

Retention and erasure policies

Our retention and erasure practices are set out in our retention schedule which is available on request from the school office

APD review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed **annually** or revised more frequently if necessary.

Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and workforce privacy notice.