FIVE RIVERS
Multi Academy Trust

DATA PROTECTION POLICY

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 GDPR, and other related legislation. 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 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 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 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 / Heads of School 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.

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 to Pupils and Parents (Principals / Heads of School are responsible for ensuring this is displayed on the academy website and handed to new parents upon induction)

Appendix 2: Privacy Notice to Staff (Principals / Heads of School 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, Principals and Heads of School are responsible for completing these during the development, testing and delivery stages of any new project.

Privacy Notice for parents and pupils: How we use pupil information

Appendix 1

Why do we collect and use pupil information?
Five Rivers Multi Academy Trust (the accountable body for Tinsley Meadows Primary Academy and Abbeyfield Primary Academy) is a data controller for the purposes of the General Data Protection Regulation 2018.

We collect pupil data and use it:

- to support pupil learning;
- to monitor and report on pupil progress;
- to provide appropriate pastoral care;
- to assess the quality of our services;
- to comply with the law regarding data sharing.

The categories of pupil information that we collect, hold and share include:

- personal information (such as name, unique pupil number and address);
- characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- attendance information (such as sessions attended, number of absences and absence reasons);
- assessment information;
- special educational needs information;
- relevant medical information;
- exclusions / behavioural information.

Collecting pupil information
Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation (GDPR), we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data
Pupil data is stored securely and retained according to the Trust's retention schedule. The retention schedule specifies the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use. Some retention periods are governed by statute; others are guidelines following best practice. Every effort has been made to ensure that retention periods are compliant with the requirements of the GDPR and the Freedom of Information Act 2000.

Who do we share pupil information with?
We routinely share pupil information with:

- schools that our pupils attend after leaving us
- the local authority
- the Department for Education (DfE)
- the school nurse and CCG/NHS

Why we share pupil information
We do not share information about our pupils with anyone outside school without consent

unless the law and our policies allow us to do so. If we require any further information about pupils or parents, we will explain the reason for this, tell you who we are sharing it with (if applicable) and we will ask the pupil or parent to sign a consent form before any information is used or shared. Once we have used your information for the purpose intended we will destroy this information swiftly and securely.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring. We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and

retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or to be given access to your child's educational record, contact the Principal/Head of School:

- Deborah Sanderson (Principal) if you are a pupil at Tinsley Meadows Academy
- Helen Best (Principal) if you are a pupil at Abbeyfield Primary Academy

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

Complaints
We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting our data protection officer.

You can also complain to the Information Commissioner's Office in one of the following ways:

- 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

Contact:
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) enquiries@fiveriversmat.uk

Tinsley Meadows:
Deborah Sanderson (Principal) enquiries@tinsleymeadows.sheffield.sch.uk

Abbeyfield:
Helen Best (Principal) headteacher@abbeyfield.sheffield.sch.uk

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

Privacy Notice:

Appendix 2

For staff of Five Rivers Multi Academy Trust

The General Data Protection Regulation 2018: How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work in our academies. This is for employment purposes to assist in the running of the academy and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector;
- enabling development of a comprehensive picture of the workforce and how it is deployed;
- informing the development of recruitment and retention policies;
- allowing better financial modelling and planning;
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body.

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to the Department for Education (DfE).

If you require more information about how we and/or DfE store and use your personal data, please refer to The Information Governance Toolkit (which is made available to all staff) or visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting our data protection officer.

You can also complain to the Information Commissioner's Office in one of the following ways:

- 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

Contact:

If you want to see a copy of the information about you that we hold, or iIf 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) enquiries@fiveriversmat.uk

Tinsley Meadows:

Deborah Sanderson (Principal) enquiries@tinsleymeadows.sheffield.sch.uk

Abbeyfield:

Helen Best (Principal) headteacher@abbeyfield.sheffield.sch.uk

Or

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

Privacy Impact Assessments - Guidance

Appendix 3A

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 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.

Privacy Impact Assessment Template

Appendix 3B

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 How will the data / information be obtained, used and retained?
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: