Data Management Policy

Our Ambition: To be the highest performing MAT in the country Our Mission: To improve the communities we serve for the better

Written by	Beverley Dale
Date for Review	November 2022
Approving Body	The Strategic Development Committee
Signed Chair of Trustees	

Vision:
Challenging educational orthodoxies so that every child makes good progress in core subjects;all teachers are committed to personal improvement and fulfil their responsibilities;
all children receive a broad and balanced curriculum;all academies strive to be outstanding.

Context

The Forge Academy Trust is committed to maintaining the confidentiality of itsinformation and ensuring that all records within the Trust are only accessible by the appropriate individuals. In line with the requirements of the UK General Data Protection Regulation (UK -GDPR), the Trust also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were originally intended.

The Trust has created this policy to outline how data is managed, stored, accessed, monitored, retained and disposed of, in order to meet the Trust's statutory requirements.

Legal framework

This policy has due regard to legislation including, but not limited to, the following:

- General Data Protection Regulation (2018)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act

1980)This policy also has due regard to the following guidance:

- Information Records Management Society 'Information Management Toolkit for Schools 2019'

Scope of the policy

This policy applies to all records created, received, or maintained by permanent or temporary staff of the trust while carrying out its functions. Also, by agents, contractors, consultants, or thirdparties' action on behalf of the trust.

Records are defined as all those documents which facilitate the business carried out by the trust and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard or electronic format e.g., paper documents, emails, skype conversations, notes of telephone calls, text messages, word documents,presentations etc.

Management Of Data Protection

The Trust has a statutory responsibility to maintain the trusts records and record keeping systems inaccordance with the regulatory environment specific to it and its academies.

Each academy has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements and this policy.

Chief Executive Officer

- To ensure that the trust adheres to any data protection legislation.
- As the data controller, the trust processes data in a secure manner.
- The trust is transparent with data subjects about how their data is processed.
- Ensures that each academy follows the data protection policies set out by the trust.

Trustees

- Policies are sent to trustees to review in line with time management structures
- Feedback to trustee board on DP
- Liaising with Trust Data Protection Lead/DPO regarding DP
- Supporting Trust Data Protection Lead with scrutiny visits
- Point of contact regarding matters with trustee board
- Update knowledge in relation to DP

Data Protection Officer

- Be the named DPO for the Trust
- Work with Trust Data Protection Lead to review/update any related policies
- Carry out annual audits of the trust/each academy
- Provide information for the trust/DP Leads through SLA e.g. webinars. Newsletters
- Carry out any necessary training
- Support trust/academies with data breaches, subject access requests etc.

Trust Data Protection Lead

- Working with the DPO to ensure that all policies are up to date.
- Liaising with the DPO to look at current compliance
- Liaising with the Head of School to ensure that policies are implemented.
- Meeting with the GDPR Leads to discuss compliance
- Carrying out scrutiny visits with each academy
- Meeting with the designated trustee regarding DP
- Reporting to CEO/Trustees regarding data protection

Academy Principals

- To oversee data protection at each individual academy.
- To meet with the Data Protection Lead to ensure that data is being processed in line with trust policies.
- To ensure that Data Protection Leads have the correct resources to undertake their role.

Data Protection Leads

- Implement DP policies of the trust
- Maintain Data Assets Inventory
- Produce Data Sharing Register
- Maintain records in line with data retention register
- Keep up to date records – Retention, destruction log, exit agreements, new starters etc.
- Communicate with staff regarding DP
- Keep data protection training Log
- Attend data protection meetings organised by
- Support with annual DP Audits
- Complete self evaluation

Staff

- Follow all trust policies in line with data protection.
- Speak to the Data Protection Lead if they have any queries relating to the processing of data.
- Uphold the trust's strong principles for data protection.
- Have the opportunity to speak to the Data Protection Officer if they have any concerns relating to how data is being processed.
- Attend all related training on data protection.

Creation and Management of School Archives

The Forge Trust archive is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage;to prompt memories of school-life among many generations of students and staff; and to serve as a research resource for all interested in the history of the trust, its academies, and the communities they serve.

Management of pupil records

Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school or academy that a pupil attends and includes all personal information relating to them, e.g., date of birth, home address, as well as their progress and achievement.

The following information is stored on the front of a pupil record, and will be easily accessible:

- Forename, surname, gender and date of birth
- Unique pupil number
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate

The following lists common and potential record types that form part of the Pupil Record:

- Admissions form
- Details of any SEND
- If the pupil has attended an early years setting, the record of transfer
- Fair processing notice – only the most recent notice will be included
- Annual written reports to parents
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the pupil
- Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan
- Any notes indicating child protection disclosures and reports are held
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g., mentalhealth
- Notes indicating that records of complaints made by parents, or the pupil are held
- Examination results – pupil copy
- SATS Results

The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in an **appropriate secure location**: they should not be forwarded to the pupils' next school

- Attendance Registers and Information
- Absence notes and correspondence
- Parental and, where appropriate, pupil consent forms for educational visits, photographs, and videos, etc.
- Accident forms (a copy can be placed on the pupil record if it is a major incident)
- Medicine consent and administering records
- Copies of birth certificates, passports, etc.
- Correspondence with parents about minor issues, e.g., behaviour
- Pupil work and drawings
- Previous data collection forms which have been superseded

Hard copies of disclosures and reports relating to child protection are stored in a securely locked filing cabinet in a securely locked room – a note indicating this is marked on the pupil's file.

Hard copies of complaints made by parents or pupils are stored in a file in an appropriate secure location – a note indicating this is marked on the pupil's file.

Actual copies of accident and incident information are stored separately on the individual academies' management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

Each academy will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.

The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, a named individual will be responsible for disposing records and will remove these records.

Electronic records relating to a pupil's record will also be transferred to the pupils' next school.

Storing and protecting information

The Data Protection Lead will undertake a risk analysis to identify which records are vital to Trust and individual academies' management and these records will be stored in the most secure manner.

Each academy will conduct a back-up of information in line with the current ICT Security – Backup Policy to ensure that all data can still be accessed in the event of a security breach, e.g., a virus, and prevent any loss or theft of data.

Where possible, backed-up information will be stored off the school premises, using a central back-up service operated.

Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records are not left unattended or in clear view when held in a location with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up.

Where data is saved on removable storage or a portable device, the device is kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors do not use their own personal email addresses for school purposes.

All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password in line with the current ICT Security – Password Policy.

Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, members of staff always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the UK GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the each academy containing sensitive information are supervised at all times.

The physical security of the Trust's buildings and storage systems, and access to them, is reviewed termly by the site manager in conjunction with the GDPR Lead. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Head of School/headteacher and extra measures to secure data storage will be put in place.

The Trust takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The DP Lead is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Accessing information

The Forge Trust is transparent with data subjects, the information we hold and how it can be accessed.

All members of staff, parents of registered pupils and other users of the Trust, e.g. visitors and third-party clubs, are entitled to:

- Know what information the Trust holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held.
- Understand what the Trust is doing to comply with its obligations under the UK GDPR.

All members of staff, parents of registered pupils and other users of the Trust, its academies and its facilities have the right, under the UK GDPR, to access certain personal data being held about them or theirchild.

Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

Digital continuity statement

Digital data that is retained for longer than six years will be named as part of a digital continuity statement.

The DP Lead will identify any digital data that will need to be named as part of a digital continuity statement.

The data will be archived to dedicated files on the Trust's servers, which are password-protected – this will be backed-up.

Memory sticks will never be used to store digital data, subject to a digital continuity statement.

The IT Provider will review new and existing storage methods annually and, where appropriate add them to the digital continuity statement.

The following information will be included within the digital continuity statement:

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information

- A description of how access to the information asset register is to be managed in accordance with the UK GDPR

Information audit

The Trust conducts information audits on an annual basis against all information held by each academy to evaluate the information the academy is holding, receiving, and using, and to ensure that this is correctly managed in accordance with the UK GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information

The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

The GDPR Lead is responsible for completing the information audit. The information audit will include the following:

- The Trust's and individual academies' data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document

The DP Lead will consult with staff members involved in the information audit process to ensure that the information is accurate.

Once it has been confirmed that the information is accurate, the DP Lead will record all details on the Trust's Information Asset Register.

The information displayed on the Information Asset Register will be shared with the Board and each designated academy leader to gain their approval.

Disposal of data

Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The DP Lead will keep a record of all files that have been destroyed.

Where the disposal action is indicated as reviewed before it is disposed, the DP Lead will review the information against its administrative value – if the information should be kept for administrative value, the DP Lead will keep a record of this.

If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

Where information has been kept for administrative purposes, the DP Lead will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

Where information must be kept permanently, this information is exempt from the normal review procedures

Monitoring and review

This policy will be reviewed on an annual basis by the DP Lead in conjunction with the Board, CEO & Trust DP Lead – the next scheduled review date for this policy is 01/01/2023.

Any changes made to this policy will be communicated to all members of staff, the board, and the local governing bodies.