



Information Governance Policy Framework

January 2026

Approved by:	Date:
Audit & Risk Committee	15 October 2025
Policy Authors:	Review Summary:
CFO Paul Withers – Trust DPO Natalie Wilkinson – Lead IG Officer	New trust policy
Links to:	
Privacy Notices Freedom of Information Publication Scheme	

Contents

1.0	Policy Statement.....	5
2.0	Purpose.....	7
3.0	What is Information Governance?	7
4.0	Applying the Policy Framework	8
5.0	Delivery	9
6.0	Information Governance Roles and Responsibilities	11
7.0	Strategic Implementation	11
8.0	Governance and Compliance	12
8.1	Employees.....	12
8.2	Trust Board	12
8.3	Others Working on Behalf of the Trust.....	13
8.4	Responsibilities.....	13
Part 1: Information Risk and Security Policy.....		14
1.1	Policy Statement	14
1.2	Scope	15
1.3	The Policy.....	16
1.3.1	Information Assets & Risk Management.....	16
1.3.2	Information Asset Security & Confidentiality	16
1.3.3	Access Controls.....	17
1.3.4	Equipment Security.....	18
1.3.5	Mobile Working.....	18
1.3.6	Timeout Procedures	19

1.3.7 Use of Removable Media	19
1.3.8 Information Classification	19
1.3.9 Posting, emailing, faxing and printing information.....	19
1.3.10 Physical and Environmental Security	21
1.3.11 Equipment and Data Disposal	21
1.3.12 Intellectual Property Rights	21
1.3.13 Systems development, planning and procurement.....	21
1.3.14 Data Changes	22
1.3.15 Cyber Security	23
1.3.16 Information Sharing	24
1.3.17 Breach Management	24
1.3.18 Business Continuity Planning	24
1.3.19 Contracts	24
1.3.20 Contracts of Employment	25
1.3.21 Personal Use.....	25
1.3.22 Social Networking and Media Platforms	
.....	25
Part 2: Closed Circuit Television (CCTV) Policy	28
Part 3: Data Protection Policy	34
Part 4: Confidentiality Policy	38
Part 5: Information Rights Policy.....	42
5.1 Policy Statement.....	42
5.2 Scope	42
5.3 The Policy.....	43
5.4 Subject Access Requests.....	46

Part 6: Records Management Policy.....	49
2 Purpose of Disposal Schedule.....	49
Section 6.3 – Definitions of Records held by Forge Brook Trust in	51
respect of its Functional Areas.	51
1. Management and Organisation	51
Section 6.4 – Electronic Records	53
Part 7: Incident Management Policy	67

1.0 Policy Statement

This Policy Framework consists of an Information Governance Strategy and seven Policies. The Information Governance Strategy, Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) sets out the legal requirements, which trusts are obliged to follow with regard to information governance and confirms the trust's commitments to these requirements. It also recognises trust pupils at the heart of its business and brings together recognition of new ways of working and developing services to better meet their needs. This Framework also establishes a culture of individual responsibility for information governance, informed and supported by awareness and training for employees, governors and others working for or on behalf of the trust. This will enable all to understand the importance of information governance, know their responsibilities, and manage information appropriately.

This Policy Framework applies to all employees, governors and anyone else working for or on behalf of the trust i.e. partners, contractors and agents.

Non-compliance with this Framework and the associated Policies could potentially expose the trust and/or its customers to unacceptable risk. Section 8 Governance and Compliance details responsibilities and consequences for non-compliance applicable to all.

To this end, the trust commits to:

- **Information Governance Management:** establishing and supporting robust operational and management accountability structures, with appropriate resources and expertise to ensure information governance issues are dealt with appropriately, effectively and at levels within the organisation commensurate with the type and gravity of the issue in question
- **Staff Empowerment:** embedding a culture of individual responsibility and capability across the council in relation to information management, protection and use as part of 'business as usual'
- **Training and Awareness:** implementing a system of training and awareness that meets government and contractual mandatory requirements, is role based, assessed and capable of equipping employees with the skills and knowledge necessary to do their jobs and respond to customer demand while complying with the Data Protection Regulations and Information Security requirements.
- **Systems and Processes:** establishing and maintaining information systems and processes to enable the efficient and secure storage and retrieval of information and the management of information risk
- **Policy and guidance:** developing and embedding, policies and guidance documents in relation to the respective areas of information governance that support employees to fully understand the standards, practices and responsibilities required within the information governance framework and to take appropriate action where necessary
- **Audit:** monitoring employee compliance with the Information Governance Policy Framework through regular audits and reports.

The Information Governance Policy Framework is addressed in three parts:

1. **Part 1: Information Risk & Security Policy** – including:
 - Confidentiality and Data Protection

- Information sharing and processing
- Data privacy and information security impact assessments
- Information and cyber security
- Incident Management Policy (Data Breach)
- CCTV Policy

2. **Part 2: Information Rights Policy** – including:

- Freedom of Information
- The Data Subjects rights, under the UK General Data Protection Regulations 2016 (GDPR) and the UK Data Protection Act 2018 (DPA).

3. **Part 3: Records Management Policy** – including Information Quality Assurance.

These Policies are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the trust and ensuring that relevant and accurate information is available where and when it is needed to improve service delivery to pupils and parents. It will also ensure that measures are in place to reduce the occurrence of breaches in information security.

This Policy Framework is owned by the Information Asset Owner (IAO) and all existing procedures relating to Information Management, Information Security, Access to Information and Records Management will now fall under this Framework

This Framework will seek to bring together all of the existing procedures, requirements, standards and best practices and review/update them as appropriate.

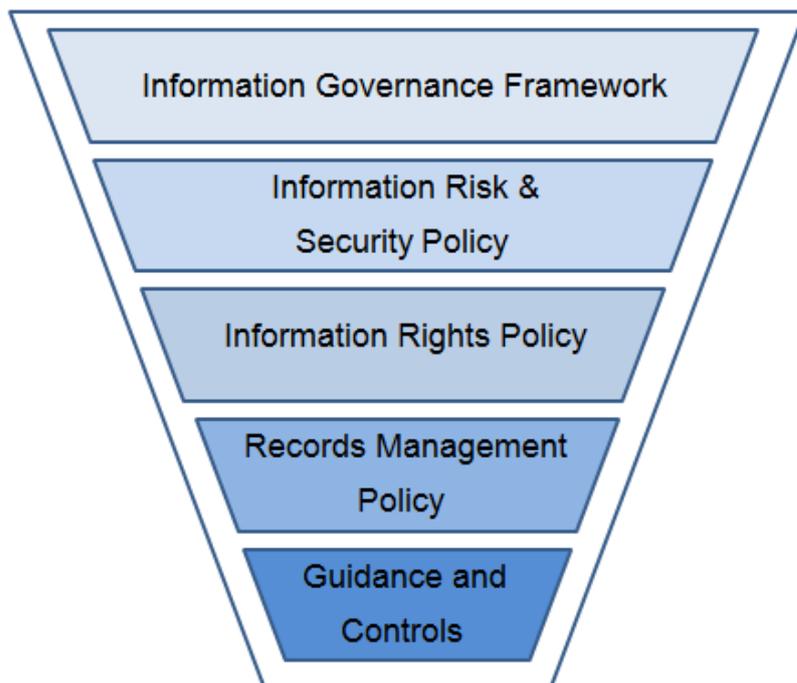


Fig 1: Information Governance Framework

2.0 Purpose

The Information Governance Policy Framework will underpin the trust's strategic goals and ensure that the information needed to support and deliver their implementation is reliably available, accurate and understandable.

Information within the trust takes many forms including data stored on computers, transmitted across networks, presented on web pages, printed or written on paper, sent by fax, stored on tapes, CDs, DVDs or spoken verbally, directly or indirectly.

Information is a vital asset for the trust, supporting both day-to-day operations and the effective management of services and resources. Information is also important in regard to improvements to service delivery and how the trust is able to respond to changing customer needs and demands. Therefore, it is essential that all trust information is managed effectively within a robust governance framework.

Successful application of this approach will lead to:

- Affective identification, management and or mitigation of information, risks, breaches and incidents.
- Appropriate and adequate processes and awareness to support the duty of confidentiality and compliance of the data protection regulations.
- Improvements in information handling and processing activities.
- Increased customer confidence in the trust and its staff with regards to information collection and processing.
- Supported sharing of lessons learnt and best practice.

3.0 What is Information Governance?

"Information governance" describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used by the trust are sourced, held and used appropriately, securely and legally. Information governance ensures appropriate controls, responsibilities and actions for the security, confidentiality and protection of information is embedded into the trusts business as usual and covers all information held by the trust (for example – pupils, parents and employees, financial and corporate) and all "information systems" (assets) used to hold that information.

Systems may be purely paper-based or partially or totally electronic. The information concerned may be "owned by" or required for use by the trust and hence may be internal or external.

As a provider of educational services, the trust carries a responsibility for handling and protecting information of many types and categories. These types of information include personal data, commercially sensitive/confidential data and non-confidential/public data

alongside business critical information.

Having accurate relevant information available at the time and place where it is needed, is critical in all areas of the trust's business and plays a key part in corporate governance, strategic risk, service development and performance improvement and overall meeting the needs of our customers. It also supports the trust's commitment to transparency and the Open Data agenda alongside the requirements for Privacy by Design (PbD).

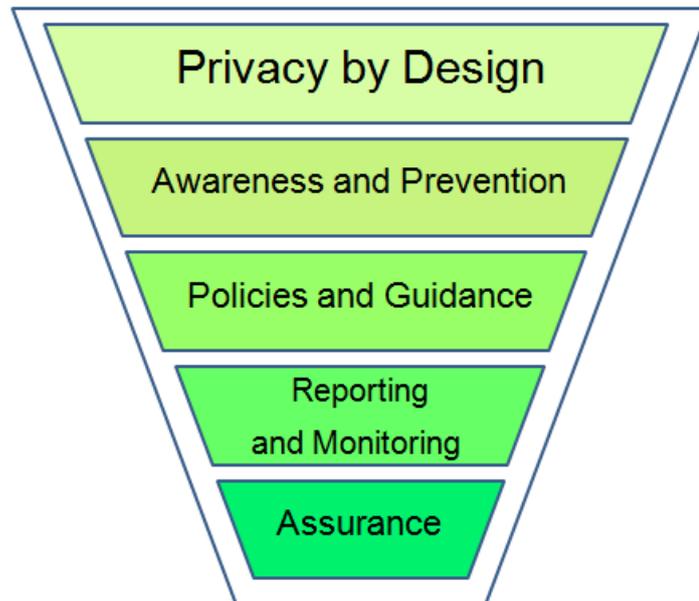


Fig 2: Privacy by Design Framework

Good Information governance will enable the trust to meet national and legal requirements.

The trust is obliged to abide by all relevant UK and European Union legislation. Appendix 1 contains a list of some of the primary sources of legislation, standards and guidance, relating to information governance with which the trust must comply.

4.0 Applying the Policy Framework

In adopting this Information Governance Policy Framework, the trust recognises and supports:

- the principle that accurate, timely and relevant information is a legal requirement and essential to deliver high quality services and that it is the responsibility of anyone working for or on behalf of the trust to ensure and promote the quality of information and to actively use information in decision-making processes
- the need for an appropriate balance between openness and confidentiality in the management and use of information
- that the principles of corporate governance and public accountability place equal importance on the confidentiality of, and the security arrangements to safeguard, both

personal information about pupils, parents and employees and commercially sensitive information

- the need to share information with other organisations in a controlled and secure manner consistent with the interests of the customer and, in some circumstances, the public interest.

5.0 Delivery

Through implementing this Framework, the trust will:

- establish robust information governance processes conforming to statutory requirements and national standards
- ensure that all practices and procedures relating to collection, processing and or sharing of personal, sensitive and trust corporate information are legal and conform to best and/or recommended practices or standards
- ensure that clear advice is given to pupils and parents about how their personal information is recorded, handled, stored and shared by the trust and its partners. The trust will also provide them with guidance, to explain their rights, how their personal information is handled, how they can seek further information and how they can raise concerns.
- ensure appropriate levels of security are applied at all times, e.g. through the use of data protection impact assessments (DPIA – formerly known as PIA) and or information security assessments.
- provide clear advice and guidance to employees and ensure that they understand their responsibilities and apply the principles of information governance to their working practice in relation to protecting the confidentiality and security of personal information and appropriate handling and maintenance of trust information assets
- maintain a clear reporting structure and ensure through management action and training that all individuals working for or on behalf of the trust understand information governance requirements alongside the duties of confidentiality and data protection.
- undertake reviews and audits of how information is recorded, held and used. Management audits will be used to identify good practice and opportunities for improvement alongside the mitigation of identifiable risks.
- ensure procedures are reviewed to monitor their effectiveness so that improvements or deterioration in information handling standards can be recognised and addressed
- ensure that when service developments or modifications are undertaken, a review is undertaken of all aspects of information governance arrangements to ensure that they are robust and effective
- work to instil an information governance culture in the trust through increasing awareness and providing training on the key issues
- ensure there are robust procedures for notifying and learning from information governance breaches and security incidents in line with the trust's Information Risk and Security Policy, which forms part of this Framework
- ensure all employees undertake the appropriate level of Information Governance Awareness training for their role on an annual basis. The requirement of any further information risk and security or records management training will be subject to the role of the individual.

There are five interlinked principles, which guide the application of this Information Governance Policy Framework:

- Quality Assurance
- Legal Compliance
- Information Security
- Proactive use of information
- Openness and transparency

To ensure **Information Quality Assurance**, the trust will:

- establish, maintain and promote policies and procedures for information quality assurance and the effective management of records
- undertake or commission assessments and audits of its information quality and records management arrangements
- ensure that key customer data is accurately recorded and maintained, including regular cross-checking against source data
- ensure that managers as Information Asset Owners (IAOs) are required to take ownership of, and seek to improve the quality of information within their services and that information quality is assured at the point of collection.
- Ensure that appropriate reports and records are maintained in line with the requirements to capture and assess processing activities.

To ensure **Legal Compliance**, the trust will:

- regard all identifiable personal information relating to pupils, parents and employees as confidential except where national requirements on accountability and openness require otherwise
- establish and maintain policies or procedures to ensure compliance with relevant law and regulation including the GDPR and UK Data Protection Act, the Human Rights Act, the Common Law Duty of Confidentiality and all associated guidance
- establish and maintain policies or procedures for the controlled and appropriate sharing of information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act) or any other requirements for data sharing in accordance with national contracts and or public tasks.

To ensure that appropriate and legal compliant **Information Security** exists, the trust will:

- establish and maintain an Information Risk & Security Policy along with respective procedures for effective policing and secure management of all its Information Assets, resources and IT systems
- undertake and/or commission assessments and audits of its information and IT security arrangements in-line with the said policy
- promote effective confidentiality and security practices to ensure all permanent/temporary, contracted employees and third party associates of the trust adhere to this via appropriate laid down policy procedures, training and information awareness schemes/documentation
- establish and maintain appropriate policing, incident reporting procedures and monitoring and investigations of all instances, actual and/or potential, along with any reported breaches of confidentiality, security or the GDPR/UK Data Protection Principles.
- Identify and classify information to ensure that it is handled and shared appropriately.
- Ensure effective reports, processes and records are in place to provide information asset owners with the ability to identify risks and take actions.

To ensure **proactive use of information**, the trust will:

- Ensure the trust embeds and monitors data protection by design by proactively assessing changes to the way we create, use, store and or share information.
- Ensure systems are in place to recognise information assets and owners.
- Ensure systems and or processes are in place to recognise, identify and take action against information risks.
- ensure information systems hold the information required to support customer focused service delivery and operational management
- develop information systems and reporting processes which support effective performance management and monitoring
- develop information management awareness and training programmes to support managers in using information to manage and develop services
- ensure that, where appropriate and subject to confidentiality constraints, information is shared with other organisations in order to support improved service delivery.

To ensure **Openness**, the trust will:

- ensure that non-confidential information about the trust and its services is readily and easily available through a variety of media, in line with the trust's FOI Publication Scheme
- implement policies to ensure compliance with the Freedom of Information Act and the Environmental Information Regulations
- ensure that customers have readily and easily available access to information relating to trust services, and their rights as service users
- have clear procedures and arrangements for liaison with the press and broadcasting media, and customers.
- Ensure appropriate Privacy Notices are in place to capture the requirements of GDPR in providing data subjects with adequate and appropriate information over the way in which the trust collects processes and shares information while ensuring the rights of individuals are clearly identified.

6.0 Information Governance Roles and Responsibilities

The Information Governance Structure in the trust consists of the following:

Information Asset owner	James Ludlow
Data Protection Officer	Paul Withers
Trusts Lead	Natalie Wilkinson
Internal trust lead	Shaun Millington
Trust Board	

7.0 Strategic Implementation

The trust will monitor implementation of this Policy Framework through regular meetings with the trust board, which will involve:

- ensuring the development and review of policies and procedures required for information

governance and having final approval of these documents.

- Ensuring appropriate resources are in place to achieve compliance of the regulatory requirements.
- Reporting on progress, incidents and issues to the trust board.

This Framework will be reviewed bi-annually or as required in response to any significant legislative changes, mandatory requirements, national guidance or as a result of significant information governance breaches or incidents and approved by the Information Asset Owner and the Trust Board

The Information Asset Owner will be a key part of this process as they are the officer accountable for information assets across the trust and are responsible for ensuring that appropriate information governance arrangements are in place locally and that national or legal requirements are met.

8.0 Governance and Compliance

Non-compliance with this Framework and relevant policies could potentially expose the trust and/or its customers to risk. The potential impact of damage or loss of information includes disruption to services, risk to citizens, damage to reputation, legal action, personal distress, loss of confidence, or media coverage and may take considerable time and cost to recover.

8.1 Employees

All new employees will receive awareness training and guidance on information governance, which will include:

- Confidentiality
- Data Protection
- Information and Cyber Security
- Information Rights

All employees will be required to repeat their information governance awareness training annually between April and March.

Employees who do not comply with these policies/procedures may therefore be subject to disciplinary action, in line with the trust's disciplinary procedures.

8.2 Trust Board

All trustees will also receive annual awareness training and guidance on information governance, which will include confidentiality, data protection, information security and cyber security alongside lessons learnt and proactive data security notices. Members' failure to comply with these policies/procedures will constitute a potential breach of the trust's Code of Conduct.

8.3 Others Working on Behalf of the Trust

Any persons working for and on behalf of the Trust must undertake appropriate awareness training prior to gaining access to trust held information or business critical data/systems. All managers are therefore responsible for ensuring that any person, agent, consultant, temporary or honorary member of staff must comply with national, legal and local information governance awareness and abide by the duties of confidentiality and data protection.

8.4 Responsibilities

The CEO shall have overall responsibility for managing and implementing the Framework and related policies and procedures on a day-to-day basis.

Managers are responsible for ensuring that their permanent and temporary employees and contractors have:-

- read and understood this Framework and the policies and procedures applicable in their work areas
- been made aware of their personal responsibilities and duties in relation to information governance
- been made aware of who to contact for further advice
- Received appropriate and up-to-date training relating to information governance.
- Abide by the trust's Code of Conduct

Non-compliance with these policies/procedures may therefore be subject to disciplinary action, in line with the trust's disciplinary procedures and or legal action if appropriate.

The following table identifies who within the trust is Accountable, Responsible, Informed or Consulted with regards to this Framework. The following definitions apply:

- **Accountable** – the person who has ultimate accountability and authority for the Framework.
- **Responsible** – the person(s) responsible for developing and implementing and reviewing the Framework.
- **Consulted** – the person(s) or groups to be consulted when the Framework is reviewed and approved
- **Informed** – the person(s) or groups to be informed throughout the approval process.

Accountable	Senior Information Risk Owner
Responsible	Data Protection Officer
Consulted	Trust Board
Informed	All individuals employed by the trust either permanently, on a temporary basis or as a contractor, and partner organisations

Part I: Information Risk and Security Policy

1.1 Policy Statement

Information is a vital asset to the trust. Forge Brook Trust is committed to preserving the confidentiality, integrity, and availability of our information assets:

- for sound decision making
- to deliver quality services
- to comply with the law
- to meet the expectations and demands of our parents, pupils and governors
- to protect our reputation as a professional and trustworthy organisation.

The purpose of the Information Risk & Security Policy is to protect the trust's information, manage information risk and reduce it to an acceptable level, while facilitating appropriate use of information in supporting customer demand and normal business activity for the trust and other organisations that it works with. Information must be accompanied by appropriate levels of security at all times. 'Appropriate' is a degree of precaution and security proportionate to the potential risk, information category and impact of loss or accidental disclosure.

The Information Risk and Security Policy will ensure an appropriate level of:

Confidentiality

To ensure the confidentiality of information is achieved, access to information is controlled and monitored accordingly based on the data category requirements, roles of individuals and processing conditions. Information is only accessible by those who require it and only disclosed lawfully where appropriate controls and assessments have been undertaken. Systems and information assets must also ensure that appropriate levels of security are in place at all times to protect the confidentiality of the data held within.

Integrity

Information must be accurate and up to date in accordance with the Data Protection Act and Regulations under GDPR alongside the rights of the individuals with regards to rectification and erasure. All information assets and systems must be assessed regularly to ensure compliance of these requirements.

Availability

Networks, systems and information assets should always be available when required to those with a justified right to access. This relates to business continuity and systems resilience, which ensure that data remains available and secured

Anyone handling personal, sensitive or confidential information must take personal responsibility and make considered judgments in terms of how it is handled whilst delivering trust services. If in any doubt members of staff and or systems users should always seek advice from the CEO or the Data Protection Officer.

The Information Risk and Security Policy will also make sure that:

- the trust establishes a culture of care and security for information.
- information is only obtained or shared when it is required
- information owned or processed by the trust is protected against un-authorized access or disclosure
- ICT equipment is protected from accidental or malicious damage
- information security risks are properly identified, assessed, recorded and managed
- Information security incidents are reported and managed appropriately.
- appropriate safeguards are implemented to reduce security risks
- legal and regulatory requirements are understood and met
- guidance and training with regards to information security is available and up- to- date.

Compliance with this policy will be achieved by:

- ensuring that all individuals who work for or on behalf of the trust are aware of and fully comply with the relevant legislation as described in this and other policies and procedures
 - Introducing a clear process for the recognition of data changes and the appropriate application and completing of data privacy impact and information security risk assessments.
 - Ensuring that any assessments identify appropriate measures for risk identification and reduction.
- introducing a consistent approach to security, ensuring that all individuals who work for or on behalf of the trust fully understand their own responsibilities and have the appropriate tools to work with
- creating and maintaining a level of awareness of the need for information security as an integral part of day to day business
- reporting and investigating all breaches of information security, actual or suspected.

1.2 Scope

This policy applies to all individuals working for or on behalf of the trust who use or have access to trust information assets, computer equipment or other ICT facilities.

The policy applies throughout the lifecycle of the information from creation through to storage, use and transfer to retention and disposal. It applies to all information including, but not limited to:

- information stored electronically on databases or applications both on site or in the Cloud

- information stored on desktop computers, laptops, tablets, smartphones, multifunction devices, approved cloud-based storage services, and removable media such as USB drives, external hard drives, and memory cards. All such storage locations must comply with the organisation's information security controls and data handling requirements.
- information transmitted on networks or via the internet and or social media platforms
- information sent by email, fax or other communications method
- all paper records including information sent out by post
- microfiche, visual and photographic materials including slides and CCTV
- spoken, including face-to-face, voicemail and recorded conversation.

1.3 The Policy

1.3.1 Information Assets & Risk Management

All trust information assets must be risk assessed and measures put in place to ensure each asset/system is secured to an appropriate level based on the measure of risk associated with it. This process will involve identifying threats and vulnerabilities (severity of impact and the likelihood of occurrence) at an individual asset level and the analysis and assessment of risks in order to make the best use of resources.

Information security risks must be recorded within a baseline risk register and action plans put in place to effectively manage those risks. The risk register and all associated actions must be reviewed at regular intervals. Any implemented information security arrangements shall also be regularly reviewed.

Overall responsibility for information security risk management will rest with the CEO but day to day management will rest with other members of the senior leadership team.

1.3.2 Information Asset Security & Confidentiality

Information risk and security management controls and procedures for all information assets will conform to the International Standard for Information Security ISO27001:2013 and the associated code of practice ISO27002:2013.

The security of all information assets must be considered at all stages of the asset lifecycle. The risks associated with handling, storing and sending information must be identified and mitigated, giving due regard to the Common Law Duty of Confidentiality. Processes for handling information assets must give regard to relevant statutory and regulatory requirements.

The trust's ICT systems, processes and infrastructure will be designed and maintained to ensure that:

- Appropriate measures are in place to protect the trust's information and systems from damage or loss due to malicious software such as viruses and or cyber-attacks.
- Information is available when required i.e. by ensuring that information and information systems are available to authorised users at point of need and

appropriate business continuity and disaster recovery processes are in place and audited regularly for functionality.

- Robust password and access control regimes are in place and maintained.
- Managers are aware of their responsibilities with regards to authorizing and monitoring systems access.

Where equipment and devices are no longer required the ICT team will ensure that devices are appropriately cleansed for reissue or destroyed in accordance with the internal processes requirements and national standards.

Equipment will not be reallocated or reissued without appropriate data cleansing in line with the government standards such as IS5 (information security standard).

External or third party systems: In addition to the above, line managers must also ensure that they follow any password and or security controls applied by third parties and that appropriate agreements or controls are in place to ensure secure access to information being shared with the trust and utilized within the network.

1.3.3 Access Controls

Individuals given access to trust information assets should only access systems that they have authority for. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems without authority to do so. Un-authorized access to information systems or information contained within a system will also be recognized as serious breach of confidentiality under the data protection regulations.

Systems access:

Formal procedures are used to control access to IT systems. Most systems employ role based access controls (RBAC) where access is granted based on a user's role and justified requirements.

Least privilege basis access (users are only granted access to parts of the network, systems or applications that their job role requires). In some cases this may result in view only access being granted unless otherwise justified and authorised.

For access to be granted, an authorised manager must contact ICT by email or using the work request process stating the access level required.

Leaving or moving:

When individuals leave the trust or move to another team it is their manager's responsibility to ensure that access is amended or accounts are disabled/deactivated. User access rights will be reviewed, monitored and audited on a regular basis (at least annually).

Password Management:

Password Management/Addition Security: Users must follow good password hygiene by creating strong, unique passwords and updating them whenever prompted. Passwords must never be shared or written down in an insecure manner. Using a long, memorable passphrase is recommended to support both security and ease of recall. Multi-Factor Authentication (MFA) wherever available

should be used to provide an additional layer of protection for accounts and systems.

Third Party Systems Access:

Third parties requiring access to trust systems for maintenance and support must sign a 3rd party access agreement before access is granted or be supervised on site by a member of ICT staff.

1.3.4 Equipment Security

To mitigate the risks of loss, damage, theft, or compromise of equipment and to protect systems from environmental threats, hazards, and unauthorised access:

The trust operates a central data centre, with additional core services hosted in the cloud. Some systems also use on-site storage located at individual school sites. Where viable and proportionate to the size and operational needs of each site, appropriate environmental protections—such as backup power, air-conditioning, and fire-suppression measures—are implemented to support system availability.

All equipment will be appropriately maintained to ensure it operates reliably, securely, and in accordance with required specifications.

Security settings and software configurations must not be altered. Any required changes must be requested through ICT and approved prior to implementation.

Security patches and software updates are applied as frequently as possible to ensure equipment remains secure, compliant, and protected against known vulnerabilities.

1.3.5 Mobile Working

Mobile working is permitted and is subject to prior approval and the following precautions must be adhered to:

- always ensure devices or information are protected appropriately in accordance with this Policy and Framework.
- always work in an appropriate environment that ensures the confidentiality and security of any information being accessed.
- never install or use unapproved software or memory devices.
- never leave mobile devices in open areas, unattended vehicles or unsecure locations.
- never provide access to un-authorised or unapproved persons.
- never remove the security or access controls applied to trust devices
- never store passwords with, or inside, devices.
- ensure devices are charged regularly and logged on and connected to the trust network at least once a month for a period of at least two hours so that appropriate patches and security updates can be applied. Report to IT if offline for a longer period so appropriate device checks can be made.
- report any loss or theft of mobile devices immediately to your direct manager and to IT.

1.3.6 Timeout Procedures

Inactive computers are set to time out after a pre-set period of inactivity. The time-out facility will clear and lock the screen.

Users must lock their computers, if leaving them unattended using the Ctrl/Alt/Delete or Windows and L keys. (see image below)

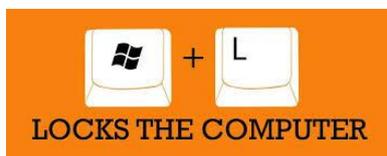


Fig 3: Quick lock Option

1.3.7 Use of Removable Media

The trust prohibits the use of any unauthorised removable media, including USB memory sticks and external hard drives. Removable media may only be used where there is a valid business need and approval has been granted.

Only encrypted removable media devices may be used to store or transfer trust data, including Sensitive or Personal Identifiable Data. Staff must ensure that encryption is enabled before any data is copied to a device. Guidance on how to encrypt removable media can be provided by ICT on request. All staff are responsible for ensuring removable media is used securely, in line with this Policy and wider data protection requirements.

1.3.8 Information Classification

All information within the trust will be identified and classified by the criteria set out in the trust's Protective Marking Procedure

This will ensure that information is given the appropriate level of protection when it is processed. Classification may change at any point in the information lifecycle e.g. a document may have a different classification when it is created to when it is approved and available for circulation. Information that is not classified will assume the lowest classification of 'Not Protectively Marked'.

1.3.9 Posting, emailing, faxing and printing information

When sending information either inside or outside the trust the appropriate method of transmission must be used according to the confidentiality or sensitivity of the information and the classification it has been given.

The risk of harm or distress that could be caused to the individual(s) that the information relates to if it were lost or sent to the wrong recipient should be considered when making the decision on the most appropriate method of transmission.

It is important that only the minimum amount of information required is sent, by whichever method is chosen.

When sending information by email the sender must:

- carefully check the recipient's email address before pressing send – this is

particularly important where the recipient fields are automatically populated by the system

- take care when using the 'reply to all' function – are all the recipients known and do they all need to receive the information being sent
- Ensure that personal, sensitive or confidential information is not included in the subject line or body of an email. If sensitive information must be sent via an unsecure email service, it must be placed in a password-protected attachment. The password must be transmitted using a completely different communication method from the original message—for example, by telephone call, text message or another secure channel. Under no circumstances should the password be sent using the same method as the attachment.
- secure email must always be used for sending personal, sensitive or confidential information if it is available
- the use of personal or home email addresses for trust business is strictly prohibited.
- when using email to communicate with other public sector network partners such as health, police or local authorities always use the approved secure email system (e.g. gcsx, gsi, cjsm etc), especially when sharing personal, confidential, sensitive information.

When sending information by post the sender must:

- ensure that the name and address details are correct – window envelopes should be used whenever possible to avoid errors in transcribing details
- ensure that only the relevant information is in the envelope i.e. the information is adequate, relevant and not excessive.
- that envelopes containing personal, sensitive or confidential information are marked 'private and confidential – addressee only'
- that a return address is added/printed on the back of the envelope

When sending information by fax the sender must:

- telephone ahead to advise the fax is being sent and ask for confirmation of receipt
- check the fax number is correct and dial carefully
- attach a cover sheet to the fax indicating who it is for, the fax number it has been sent to, the contact details of the sender, the date and number of pages (including the cover sheet) in the document
- if the information is particularly sensitive (and it cannot be sent by a more secure method) consider sending a test fax to ensure it reaches the correct recipient

When printing or photocopying information always ensure that:

- secure printers are used wherever possible
- if unsecure printers are to be used, only ever print the minimum required.
- prints are always collected immediately
- check the document to ensure you have collected every print out
- ensure the printer has enough paper to complete your print
- ensure multiple documents are separated accordingly to avoid misfiling

1.3.10 Physical and Environmental Security

Depending upon the function and the nature of use, offices where information is held will be equipped with appropriate security controls e.g. CCTV, entry controls etc. Public areas, deliveries etc. will be isolated from information processing areas.

Offices that deal with personal and/or sensitive information will have entry controls and lockable storage facilities.

ID cards, keys and other entry devices must be returned when access is no longer required.

All visitors must have official identification passes issued by the trust or school. If temporary access to systems is given a 3rd party access agreement must be signed and access must be disabled when the visitor leaves. Visitors should not be afforded opportunity to view computer screens or printed documents without authorisation.

Strangers in office areas without an ID badge should be challenged or reported. Tailgating is not permitted.

Anyone handling personal, sensitive or confidential information is required to clear paperwork from their working area when leaving it for any length of time and always at the end of each working day Paperwork should be locked away securely.

1.3.11 Equipment and Data Disposal

If a device has ever been used to process trust data, action must be taken to ensure data is irrevocably removed as part of the disposal process. All equipment that is past its useful life must be returned to ICT for disposal. The trust has a documented procedure for the disposal of equipment.

1.3.12 Intellectual Property Rights

All users must ensure that only licensed software issued or approved by ICT is installed on trust equipment. The loading and use of unlicensed software on trust computing equipment is not permitted. All users must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate license to prove the software was legally acquired. The trust monitors the installation and use of software. Any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the trust's disciplinary procedures.

1.3.13 Systems development, planning and procurement

All system developments must comply with the trust's ICT Strategy. Security and risk management issues must be considered and documented during the requirements and procurement phases of all procurements and developments which affect data relating to trust activity, trust customers, partners, employees or suppliers.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. The General Data Protection Regulations (GDPR) has introduced a legal requirement for Data Protection Impact Assessments and privacy by design in certain circumstances.

The trust will, therefore, ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout the project lifecycle. Projects would include (but not limited to):

- A new IT system
- A new data sharing initiative
- A proposal to identify people in a particular group or demographic
- Using existing data for a new or more intrusive purpose
- Introduction of a new CCTV system or the application of new technology to an existing system

IT systems are checked both internally and by external accredited suppliers on a regular basis for security and technical compliance with relevant security implementation standards.

1.3.14 Data Changes

In order to gain assurance that information is handled securely, legally and in line with any legislation or IG requirements the inclusion of Information Governance and Privacy must be taken into account at the beginning of new projects or processes that affect the way in which information is handled.

Staff must not purchase new systems, mobile technology devices, and external services or implement process changes that involve the use, creation, storage and or sharing of personal, sensitive or confidential data without first obtaining approval from the Headteacher.

Depending on the information you provide the CEO or Headteacher may ask you to complete:

- Information Security Assessment (ISA)
- Data Protection Impact Assessment (DPIA)
- Site or Premises Assessment form

Where data processing is involved it may also be necessary to ensure that IG or DPA (Data Protection Act) clauses are included in contracts and or sharing, processing agreements.

The CEO undertakes assessments to provide assurance that all personal/confidential information is secure in accordance with the GDPR, DPA and DSP Toolkit requirements.

Next Steps:

Please make sure you consider the following points before ordering, buying or making changes to the way in which data is held or collected within the trust:

- Is this something that includes the storage or use of service user/staff information?
- Are you changing a process, contract or Service Level Agreement (SLA) that involves service user/staff information?
- Are you purchasing something that will be used for the processing of service user/staff information?

- Are you purchasing something that will be used for the processing of business information?
- Is a third party organisation going to be processing any personal or special category (sensitive) data on your behalf?
- Have you contacted the CEO/Headteacher/Data Protection Officer to make them aware of your project?

If you have answered yes to any of the above questions, then you will need to obtain approval from the CEO/Headteacher.

1.3.15 Cyber Security

Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the trust. In the event of a successful attack this may also result in loss of data, potential for monetary penalties and additional replacement systems or equipment costs to rectify any data losses or disclosures and or systems functionality.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services.

Foreign states, criminals, hackers, insiders and terrorists all pose different kinds of threats. They may try to compromise public sector networks to meet various objectives that include:

- financial gain
- attracting publicity for a political cause
- controlling computer infrastructure to support other nefarious activity
- disrupting or destroying computer infrastructure stealing sensitive information to gain economic, diplomatic or military advantage

Trust employees can also be targets for criminal activity.

As with most trusts and trusts, Forge brook Trust relies heavily on access to the internet and to information held in its systems. There are several IT systems/services that have an internet presence e.g. the trust website or the ability to work from home and there are several different ways gain access to information e.g. Wi-Fi, physical networking, mobile phones, tablets etc. All can present threats to cyber security. It is widely acknowledged that it is not currently possible to keep out all attacks all of the time, but trust employs a range of tools and good practice to minimise the risk to its information and systems.

The trust has clear procedures and guidance on Information Security, which provide information on a range of areas including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Removable Media

- Sharing and disclosing information

The trust ensures that all staff receive annual cyber security training based on National Cyber Security Centre (NCSC) guidance for schools, with further training and updates provided as necessary to address emerging risks and changes in best practice.

New systems and services are designed and implemented with guidance and advice from appropriate technical specialists to ensure security is considered from the outset.

To maintain the security and resilience of its infrastructure, the trust also ensures that regular penetration testing and external security audits are carried out by accredited third-party providers.

1.3.16 Information Sharing

This policy supports effective and appropriate information sharing across the trust and with partner organisations as part of overall service improvement. Sharing of information with partners is subject to appropriate information sharing/processing agreements and the requirements of the GDPR and Data Protection Act. Information sharing with other external organisations should also be supported by a purpose specific information sharing/processing agreement. All agreements should be made in consultation with the CEO/Head Teacher and Trust Board.

1.3.17 Breach Management

The trust's Procedure for Reporting and Managing Data Breaches must be followed wherever there is any un-authorised or unlawful disclosure, loss, damage or destruction to personal or confidential information. Anyone granted access to trust information is responsible for reporting any actual or suspected breach as soon as it is discovered and must be aware of the procedure and the reporting requirements.

1.3.18 Business Continuity Planning

All systems and information assets will have threats and vulnerabilities assessed by system owners to determine how critical they are to the trust. The trust's business continuity planning process will include consideration of information security gained from the information asset and risk register.

1.3.19 Contracts

If contracts involve exchange of personal or sensitive data a DPIA must be completed and approved and if services are hosted elsewhere a Technical Assessment must also be completed and approved as part of the procurement process.

Prior to award of a contract a Data Processor Agreement or Contract must be implemented and signed by any 3rd party handling personal information on behalf of the trust providing assurance that they comply with the GDPR and the Data Protection Act

requirements if processing relate to personal or special category (sensitive) data.

All new contractual arrangements with suppliers of goods or services to the trust will contain confirmation that the suppliers comply with all appropriate information security policies and procedures in accordance with the guidance on contractual clauses as provided by the Information Commissioners Office.

1.3.20 Contracts of Employment

Information security expectations of employees shall be included within job descriptions and person specifications where appropriate.

Pre-employment checks will be carried out in accordance with relevant laws and regulations and proportional to access to information and business requirements this may involve requirements for BPSS/DBS checks.

Employee security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Annual information governance training is a national legal requirement that the trust must comply with.

1.3.21 Personal Use

Personal use of trust ICT equipment is permitted providing that it is in line with the provisions of the Email and Internet Usage Procedure and other procedures relating to the use of trust devices.

1.3.22 Social Networking and Media Platforms

In order for the trust to improve its accessibility and visibility on social media sources, a policy and supporting guidance is required to ensure that any regulatory or professional, legal requirements are fully understood and met.

This policy provides staff with clear guidelines on:

- acceptable use of social media linked to their employment
- acceptable use of social media for the purpose of trust business
- being mindful of any content they share on such platforms
- maintaining appropriate standards of confidentiality
- maintaining and protecting professional boundaries with service users

The use of social media for and in private are not covered within this policy as all staff must follow professional codes of conduct, employment contracts and trust policies at all times.

Trust employees will not use or maintain a social networking site that contains:

- Personal identifiable information of trust service users and/or their relatives

- Personal identifiable information of other trust employees in relation to their employment, including judgements of their performance and character
- Photographs of other trust employees or service users taken for the purpose of social networking without full and explicit consent in line with the consent guidance.
- Statements that bring the trust, its services, its staff or contractors into disrepute
- Trust confidential or business information must not be loaded onto a private or business social networking site without the appropriate senior managerial sign off and without compliance of the Trust publication scheme.
- Employees must examine carefully any email or message coming from social networking sites or contacts, as these may be unreliable, contain malicious codes, be spoofed to look authentic, or may be a phishing email
- Employees should not conduct themselves in ways that are detrimental to the trust.
- Employees should take care not to allow their interaction on these websites or platforms to damage working relationships between members of staff and service users.

Information security is implemented to protect and provide adequate security levels for information containing personal, sensitive and or confidential information relating to an individual or the business. It is vital that Social Networking forms part of this policy and supports this policy in order to protect the organisation, its staff and ensure that at all times the trust is fully compliant with any Data Protection Regulations or legal requirements.

There are 3 main elements for the use of social media sites within trust services or functions:

Permission:

- Teachers and managers must gain approval from the CEO/Head Teacher for the creation and or use of social media sites and outlets.
- Un-authorized use of social media to promote the trust is a breach of these policies and will be managed in line with trust disciplinary proceedings and potential dismissal or suspension.

Integrity

- Ensuring that information is accurate and can be modified by authorised persons only
- Staff must follow policies for the use of a social network, site or any external web application.

Accountability

- The senior leadership team are responsible for ensuring that those using social media to support services as part of a business function, comply at all times with the required and appropriate policies, procedures and codes.

This will ensure that the trust complies with legislation and standards relating to the use of social media, including the Computer Misuse Act, ISO27001 (International Standards for Information Security) and the Confidentiality Code of Practice: Information Security Management.

Part 2: Closed Circuit Television (CCTV) Policy

2.1 Policy Statement

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at our trusts.

- The CCTV system is owned or leased by the trust or by individual schools within the trust. Its deployment is determined by the trust and school leadership teams to ensure it meets the operational, security and safeguarding requirements of each site.
- The CCTV system consists of a range of cameras and associated storage equipment installed at appropriate locations across trust sites. The specific types and placement of cameras and storage servers are determined according to the operational and safeguarding needs of each school.

Monitoring of CCTV footage is carried out locally by authorised personnel within each school, as designated by the trust or the individual school's leadership team.

- All authorised operators and employees with access to live or recorded CCTV images must handle and view such footage strictly in accordance with relevant legislation, trust policies, and recognised codes of practice. All operators receive appropriate training from authorised trust or school management personnel in their responsibilities, including the correct procedures for accessing, reviewing, and using CCTV footage. Staff are made aware of the restrictions that apply to the access, use, and disclosure of recorded images.
- Any changes to CCTV monitoring will be subject to consultation with staff and the trust governors.
- This policy follows Data Protection Act 2018 (DPA) and General Data Protection Regulations (GDPR) 2016 guidelines.
- The trust's CCTV Scheme is registered with the Information Commissioner under the terms of the DPA 2018 and the GDPR 2016. This policy outlines the trust's use of CCTV and how it complies with UK and other relevant legislation.
- The policy will be subject to review to include consultation as appropriate with interested parties.

2.1.0 Scope

The system has been installed by the trust/schools with the primary purpose of reducing the threat of crime generally, protecting our premises and helping to ensure the safety of all of our staff, students and visitors consistent with respect for the individuals' privacy

- To increase personal safety of staff students and visitors and reduce the fear of crime
- To deter those with criminal intent and protect the trust buildings and their assets
- To assist in the prevention and detection of crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property

- To assist in managing the trust
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

2.1.1 Definitions

Term	Definition
Personal data	<p>The UK General Data Protection Regulation (GDPR) only applies to organisations' use of personal data. This is any information relating to an identified, or identifiable, person.</p> <p>This may include information such as the person's:</p> <ul style="list-style-type: none"> • Name • Contact details • Identification number • Online identifier, such as a username <p>It may also include anything relating to the person's physical and mental health, genetics, finances, or their physiological, cultural, or social identity.</p>
Special categories of personal data	<p>Personal data which is considered to be more sensitive and therefore requires further safeguards:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data where used for identification purposes (such as fingerprints, retina and iris patterns) • Health – physical or mental • Sex life or sexual orientation • Criminal offences and procedures
Processing	<p>Anything operation or set of operations performed on personal data including: collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.</p>
Data Subject	<p>The identified or identifiable individual to whom the personal data</p>

	relates (e.g. all your pupils, staff members will be data subjects).
Data Controller	A person or organisation that determines the purposes and means of processing of personal data (e.g you as a trust)
Data Processor	An external person or organisation, who is not employed by your trust, who processes the personal data on your trust's behalf (e.g. your payroll provider, an external careers advice service, or your parental communications provider).
Data Protection Officer	The person in your trust, or an external data protection adviser, who takes responsibility for monitoring data protection compliance.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, un-authorized disclosure of, or access to personal data.

2.2 CCTV

2.2.0 Statement of Intent

The CCTV Scheme will be registered with the Information Commissioner under the terms of the DPA 2018 and will seek to comply with the requirements of the DPA, GDPR and the Commissioner's Code of Practice.

- The trust will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.
- Cameras will be used to monitor activities within the trust and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well being of the trust, together with its visitors
- Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.
- Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained, as set out in the Regulation of Investigatory Power Act 2000.
- Materials or knowledge secured as a result of CCTV will not be used for any co - investigation of a specific crime and with the written authority of the police. Recordings will never be released to the media for purposes of entertainment.
- The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
- Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the trust CCTV.

2.2.1 Covert Monitoring

The trust may allow police to install covert cameras in trust for a specific authorised purpose subject to the police acting in accordance with the Regulation of Investigatory powers (RIPA). For example:

Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;

Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from the Headteacher or Deputy Headteacher.

Covert monitoring must cease following completion of an investigation.

Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets, unless there is a serious need for this.

2.2.2 Operation of the System

The CCTV Scheme is administered and overseen by the Trust and the Headteachers of individual schools, or their nominated representatives, in accordance with the principles and objectives set out in this Code of Practice.

Day-to-day management of the CCTV system is carried out by authorised staff, including members of the Senior Leadership Team, Business Managers, Site Managers and other designated trust personnel, as appropriate to each site.

Access to CCTV controls, hardware and recorded images is strictly limited to authorised staff or approved third-party specialists acting on behalf of the trust.

The CCTV system operates 24 hours a day, every day of the year.

2.2.3 Controls and Hardware

- The system is checked regularly to ensure it is functioning correctly, including confirming that all cameras are operational and that recording equipment is working as expected.
- Access to the CCTV controls and hardware is restricted to authorised trust or school staff, as designated by the trust.
- Unless an immediate response to events is required, staff must not direct cameras at an individual or a specific group of individuals.
- Visitors and other contractors wishing to access the CCTV controls and hardware devices will be subject to particular arrangement as outlined below.
- CCTV Operators must satisfy themselves over the identity of any visitors and other contractors wishing to access the CCTV controls and hardware devices and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be endorsed in a log book.
- It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the Site Manager, or his deputy and must be accompanied by him throughout the visit.

- Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- If out of hours emergency maintenance arises, the trust must be satisfied of the identity and purpose of contractors before allowing entry.
- A visitor's record will be maintained at trust reception. Full details of visitors including time/data of entry and exit will be recorded.
- Other administrative functions will include maintaining hard disc space, filing and maintaining occurrence and system maintenance logs.
- Emergency procedures will be used in appropriate cases to call the Emergency Services.

2.2.4 Access to CCTV Images

Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.

A **record book or digital access register** will be maintained by the responsible person at each site or by other authorised staff. This register will record all incidents and any access to or searches of CCTV footage. Each entry should include details of what was accessed and by who and how long this should be stored for.

2.2.5 Storage & Retention of CCTV Images

Recorded CCTV data will be retained only for as long as is necessary to fulfil its original purpose. In most cases this will be for a short, defined period; however, footage may be retained for longer where required for an ongoing investigation, safeguarding concern, disciplinary process, legal claim, Health and Safety Executive (HSE) enquiry, or any other situation where extended retention is legally or operationally justified.

While retained, the integrity and security of the recordings will be maintained to preserve their evidential value and to protect the rights of individuals whose images are captured.

All retained data will be stored securely on the trust's systems with strictly controlled and limited access.

2.3 Breaches of the Code (including major breaches of security)

Any breach of the Code of Practice by trust staff will be initially investigated by the Headteacher, in order for him/her to take the appropriate disciplinary action. Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

2.4 Complaints

Complaints and enquiries about the operation of CCTV within the trust should be directed to the Headteacher in the first instance.

2.5 Further information

For further information on CCTV and its use is available from the following:

- CCTV Code of Practice (published by the Information Commissioners Office)
- For further guidance from the ICO click [here](#).
- Data Protection Act 2018
- General Data Protection Regulation 2016

Part 3: Data Protection Policy

3.1 Policy Statement

Forge Brook Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the trust. This 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 information to ensure that the trust complies with its statutory obligations.

Trusts have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Trusts also have a duty to issue a Privacy Notice to all pupils/parents, which summarises the information held on living individuals, why it is held and the other parties to whom it may be passed on.

The member of staff responsible for data protection is Shaun Millington. However all staff must treat all information in a confidential manner and follow the guidelines as set out in this document. The Data Protection officer (DPO) for the trusts is:

Paul Withers, Resources & Transformation, Civic Centre 3rd Floor (HR Suite), Walsall Council, Darwall Street, Walsall, WS1 1TP.

Email Address: Informationmgmt@walsall.gov.uk

Contact Telephone Number: 01922 650970

The trust is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them. The requirements of this policy are mandatory for all staff employed by the trust, any third party contracted to provide services as well as trustees/governors and volunteers working in the trust.

3.2 Scope

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) 2016, and other related legislation. It will apply the requirements to 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.

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.

3.3 What is Personal Information?

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

3.4 Data Protection Principles

Forge Brook Trust will collect and process personal data in compliance with the data protection principles under Article 5 of the GDPR. This means personal data shall be:

- **Processed lawfully, fairly and in a transparent manner** – we evidence and explain what is being collected, why is it being collected, and how will it be used, who will it be shared with. We do this through the trust privacy notice.
- **Collected for specific, explicit and legitimate purposes** – we will collect data for a legitimate purpose only.
- **Adequate, relevant and limited** – we will only collect what is needed and nothing more
- **Accurate and kept up-to-date** – We will ensure data is accurate and is kept up-to-date
- **Storage Limitation** – We will only keep data for as long as is necessary and in accordance with relevant legislation. How we do this can be found on the trust retention policy
- **Security of information processed** – the trust will protect against un-authorized or unlawful processing and against accidental loss, destruction or damage.

Forge Brook Trust also recognizes the rights of individuals in respect of information the trust holds about them. Any requests to recognize these rights will be fully considered and evaluated so that the individual can be informed whether they can/cannot exercise the rights under their particular circumstances. These rights are:

- Right to be **Informed** – about how their data is being used
- Right of **Access** – to be able to access their data
- Right to **Rectification** – right to correct information about them that is incorrect
- Right to **Erasure** – to have their data erased when they no longer want it to be used
- Right to **Restrict Processing** – to restrict how their data is used
- Right to **Data Portability** – to move their data from one organisation to another
- Right to **Object** – to object to their data being used at all
- Right to not to be subject to **Automated Decision making, including Profiling** – sole automated decision making (where there is no human involvement) and profiling are restricted under the GDPR. The restriction can be lifted under three circumstances; (1) For a contractual basis; (2) For a legal basis; (3) based on individual's explicit consent.

3.5 Privacy Notice

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

There may be circumstances where the trust is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, Department of Education or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of our trust shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them. Under no circumstances will the trust disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the trust or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed

For full details of our privacy notice please click on the following link [Policies - The Forge Brook Trust](#)

3.6 Data Security

In order to assure the protection of all data being processed and make informed decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO. Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

3.7 Objections to Processing

Individuals have the right to request that the processing of information about them be restricted or ceased if they believe the information to be inaccurate or being held unnecessarily. The trust must investigate any such request and rectify if necessary. The Data Subject should be informed before any restriction is lifted.

3.8 Sharing Personal Data with Third Parties

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**
If a pupil transfers from a Forge Brook Trust school to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new trust. This will support a smooth transition from one trust to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.
- **Examination authorities**
This may be for registration purposes, to allow the pupils at our trust to sit examinations set by external exam bodies.
- **Health authorities**
As obliged under health legislation, the trust may pass on information regarding the health of children in the trust to monitor and avoid the spread of contagious diseases in the interest of public health.
- **Police and courts**
If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- **Social workers and support agencies**
In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- **Educational division**
Trusts may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Subject access requests should be made in writing to: Data Protection Lead, Forge Brook Trust on dataprotection@forgebrook.co.uk

Alternatively you can complete a subject access request form. This can be found at [The Forge Brook Trust](#)

3.9 Photographs and Video

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in trust only.

Unless prior consent from parents/pupils/staff has been given, the trust shall not utilise such images for publication or communication to external sources.

It is the trust's policy that external parties may not capture images of staff or pupils during such activities without prior consent. Parents are allowed to take photos of their child during such activities if it is only for their personal use. Where the image of another child is captured in the photo, it is prohibited for parents to make these public or post on social media.

Part 4: Confidentiality Policy

4.1 Policy Statement

Forge Brook Trust understands that the safety, wellbeing and protection of pupils is of paramount importance. With this in mind, all pupils must be able to expect certain levels of trust when sharing personal information with trust staff.

Pupils need to know that they can seek help from the trust in a safe and confidential manner. This policy guides trust staff and visitors on the policy and procedures surrounding confidentiality. Staff members adopt a supportive and accepting attitude towards pupils as part of their general responsibility for pastoral care. It is our hope that pupils and parents/carers feel free to discuss any concerns and worries they have, that may affect educational progress with members of the trust team.

4.2 Scope

The Pupil Confidentiality Policy aims to:

- Promote a supportive and accepting ethos within the trust.
- Safeguard the well - being of pupils
- Build trust between pupils and staff
- Empower pupils to exercise control over their situation and voice their concerns
- Prevent the trust dealing with each disclosure in isolation

4.3 Legal Framework

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

- The Education Act 2011
- The Data Protection Act 2018
- The Human Rights Act 1998
- The Freedom of Information Act 2000

This policy will be implemented in conjunction with the following trust policies:

- Data Protection Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Whistleblowing Policy

4.4 Definitions

For the purpose of this policy, 'confidentiality' is an understanding that any information shared with someone in trust will only be passed on to a third party with the prior agreement of the person disclosing it.

For the purpose of this policy, 'disclosure' is the sharing of any private information, but which is not solely in relation to child protection issues. Disclosure of the contents of a conversation may be discussed with professional colleagues, but the confider is not identified except in pre-determined circumstances.

The Designated Safeguarding Lead is a designated staff member responsible for ensuring the trust's Child Protection and Safeguarding Policy is implemented by the entire trust community, which ensures the wellbeing and protection of pupils.

At Forge Brook Trust the Headteacher, or a member of the Senior Leadership Team, of each school is the Designated Safeguarding Lead but there are a number of Designated Deputy Safeguarding Leads across trust .

4.5 Policy Application

This policy deals with personal information that may be divulged during the course of a trust day. It is not meant to deal with certain extreme situations where there is an urgent need for the disclosure of information to relevant bodies. In extreme situations, such as medical emergencies, staff members will pass on information as necessary for the wellbeing of the pupil.

All information about an individual pupil is private and will only be shared with staff members who have a legitimate need to know. All data is processed and held in line with the trust's Data Protection Policy.

The Designated Safeguarding Lead is responsible for referring the pupil's confidential information to multi-agency support services. Staff members may not make pass on confidential information unless they believe a child protection referral to the police or social services is necessary and the Designated Safeguarding Lead does not agree.

4.6 Limits of Confidentiality

In practice, there are few situations where absolute confidentiality can be offered. The trust aims to strike a balance between confidentiality and trust, and ensuring the safety, wellbeing and protection of its pupils. In almost all cases of disclosure, limited confidentiality is on offer. The professional judgement of a teacher, counsellor or health professional is vital when considering whether to inform a pupil that a disclosure may be made in confidence, and whether such confidence could remain having heard the information.

4.7 Classroom Confidentiality

It is made clear to pupils that the classroom is not a place to disclose confidential, personal information. Pupils are made aware that a staff member is always available to talk to them in private when needed. If a visitor to the classroom is contributing to the lesson, they will work within the same boundaries of confidentiality as the teacher.

4.8 One to One Disclosures

Staff members will make it clear to pupils that they may have to pass on some information if they believe the pupil is at risk. When concerns for a pupil come to the attention of staff, e.g. through observation of behaviour, injuries or disclosure (however insignificant these might appear), the

member of staff always discusses the issue with the Designated Safeguarding Lead as soon as possible.

In accordance with each school's Child Protection and Safeguarding Policy, more serious concerns, such as those involving potential abuse, are immediately reported to ensure that any intervention necessary to protect the pupil is accessed as early as possible.

4.9 Disclosures to Health Professionals

Health professionals, such as the school nurse, may give confidential information to pupils, provided the information is in regards to the pupil's wellbeing, and they are competent to do so and follow the correct procedures. The school nurse is skilled in discussing issues and possible actions with young people. On a need-to-know basis, the trust nurse may share information with appropriate staff in to enable improved support for pupils.

4.10 Breaking Confidentiality

When confidentiality must be broken because a pupil may be at risk of harm, in accordance with our Child Protection and Safeguarding Policy, the trust will ensure the following:

- Pupils are told when the information has been passed on
- Pupils are kept informed about what will be done with the information
- To alleviate their fears about everyone knowing, pupils are told exactly who their information has been passed on to

The Designated Safeguarding Lead is to be informed of any child protection concerns. Staff members are contractually obliged to immediately inform the head teacher.

Staff members are not obliged to inform the police on most matters relating to illegal activity, such as illegal drugs or assaults; instead, these are assessed on a case-by-case basis with the support of the senior leadership team.

Staff members are not permitted to pass on personal information about pupils indiscriminately.

4.11 Guidance for Teaching Staff

The safety and protection of the pupil is the paramount consideration in all confidentiality decisions. Staff members are not obliged to break confidentiality unless there is a child protection concern. Staff members are encouraged to share their concerns about pupils in a professional and supportive way. In extreme cases, staff in breach of this policy may face disciplinary action, if it is deemed that confidential information was passed on to a third party without reasonable cause.

The following principles are adhered to when supporting pupils:

- Personal matters are discussed in an appropriate time and place
- Pupils with concerns are spoken to in confidence as soon as possible
- Where there are child protection concerns, the pupil is always spoken to in confidence before the end of the trust day

- Pupils are told, prior to disclosures, that a staff member cannot guarantee confidentiality if they think a pupil is being hurt by others, hurt themselves, or hurt someone else
- Pupils are not interrogated or asked leading questions
- Pupils are not placed in the position of having to repeat the disclosure to several people
- Pupils will be informed before any information is shared
- Where appropriate, pupils are told to confide in their parents/carers

Staff members may find themselves dealing with highly personal issues and potentially upsetting disclosures. With this mind, staff members are encouraged to seek help from the Designated Safeguarding Lead or Deputy Safeguarding Leads if they are unsure about how to respond to a situation. The trust has access to several external agencies that specialise in providing advice and support.

4.12 External Visitors

All external visitors are made aware of the Confidentiality Policy and work within its limits when interacting with pupils. Healthcare professionals work within their codes of confidentiality when delivering their services within the trust.

4.13 Informing Parents/Carers

The trust works with parents/carers to create a partnership of trust. It endeavours to inform parents/carers of their child's progress and behaviour. When a pupil discusses a personal matter with a staff member, they are encouraged to share the information with their parents/carers, unless there is an identifiable child protection risk associated.

Where a staff member believes a child protection risk is posed in regards to the family of the pupil, following a disclosure, the staff member will immediately contact the Designated Safeguarding Lead and local safeguarding officer.

4.14 Dissemination

All parents/carers are made aware of the trust's Pupil Confidentiality Policy and are informed that a copy can be viewed at the trust office and on the trust website. Parents/carers are made aware that the trust cannot offer complete confidentiality if they deem a pupil is at risk from harm.

Part 5: Information Rights Policy

5.1 Policy Statement

Forge Brook Trust is fully committed to transparency, whilst recognising the need for an appropriate balance between openness and maintaining the security and (where necessary) the confidentiality of the information which it holds. It uses an assumption of full disclosure as a starting point for considering all requests for information. Information will only be withheld where there is a genuine and justifiable reason for doing so that can be supported by legislation.

Forge Brook Trust also recognises the rights of individuals in respect of information the trust holds about them. These rights are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Anyone can make a request for information held by the trust under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. Requests for personal information can also be made by the individual the information relates to under the GDPR. The trust will comply with:

- The terms of the freedom of information Act 2000 and any other relevant legislation to ensure requests for access to information held by the trust are treated in a manner that is fair and lawful.
- Walsall Metropolitan Borough Council advice and guidance.
- Information and guidance displayed on the Information Commissioner's website: <https://ico.org.uk/>

This policy should be used in conjunction with the trust's **Internet Use Policy** and **Data Protection Policy**.

5.2 Scope

This policy relates to all parts of the trust and all information created and received by the trust, regardless of media or format. This includes all paper-based records as well as information that exists, or will exist, solely in electronic form, audio/visual records and photographs.

5.3 The Policy

5.3.1 Freedom of Information (FOI)/Environmental Information Regulations (EIR)

Making a request

To be valid FOI or EIR, requests;

- must be in writing and be legible – FOI only
- can be oral or legible when written – EIR
- must clearly describe the information being sought;
- can be made by an individual or an organisation;
- must contain a name and a return address (this does not need to be a postal address but could be, for example, an email) and
- can be sent to / received by any part of the trust

To be valid EIR/FOI requests they **do not**;

- have to be written in a special form
- need to mention the FOI Act; or need to refer to “Freedom of Information”
- need to mention the EIR; or need to refer to the “Environmental Information Regulations”

5.3.2 Environmental Information Regulations

Definition

Environmental Information Regulations (EIR) cover the following information;

1. The state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements;
2. Factors, such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a);
3. Measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b) as well as measures or activities designed to protect those elements;
4. Reports on the implementation of environmental legislation;
5. Cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c); and

6. The state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures in as much as they are or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c).

The trust recognises that there are many similarities between the two regimes and that requests for “environmental information” must be answered in accordance with the EIRs rather than the FOI Act. Requests made under the Environmental Information Regulations will be handled in the same way as those under FOI, with due reference to the provisions of those Regulations.

It is possible that in some cases both regimes will be relevant. The trust will, when responding to such requests for information, endeavor to clearly identify which parts of the information fall under which regime. The trust will also seek to ensure that where requests for information are made and form part of everyday service delivery they are treated as ‘business as usual’ and not considered as valid requests under the EIR /FOI Act.

5.3.3 Data Gathering and Storage

- Information will only be gathered and stored for specified purposes.
- In order to be able to respond to requests for information the trust will implement effective records management policies to enable staff to identify whether data is held and, if it is, locate it quickly and easily.
- The trust’s retention policies will be based on the guidance in the Information and Records Management Society’s Records Management toolkit for trusts and will be reviewed regularly in line with any updates to this toolkit.
- Information held by the trust will be regularly reviewed with a view to archiving or destruction, where appropriate.

5.3.4 Publication Scheme

The trust will adopt and publish the appropriate model publication scheme, as recommended by the DfE, Information Commissioner and Walsall Metropolitan Borough Council, and approved by the trust board.

5.3.5 Dealing with Requests for Information

- Theoretically any request for information is a request under the Freedom of Information Act, however this trust has taken the decision that it will not consider any request that forms part of the normal pattern of work to be a Freedom of Information request. Only those requests which are considered to be outside the normal remit of the service provided will be recorded as Freedom of Information requests.
- The trust will assist applicants in making their request to have access to information held by the trust.
- Assistance will be given to applicants whose requests need to be transferred to another public authority (e.g. trust, council, hospital).

- The trust will exercise its duty to confirm or deny the existence of requested data, subject to any exemptions that may apply.
- The trust will supply data requested within 20 working days (or in line with the Information Commissioner's current policy during trust holidays), subject to any exemptions that may apply, and the estimated cost of complying with the request falling within the current defined charge limit. All requests for information will still be dealt with in compliance with the 20 working day deadline, whether they are recorded as Freedom of Information requests or not.
- If a response will take longer than 10 working days to respond an acknowledgement will be sent to the person making the request, informing them when the information will be supplied. We recognise this does to allow the trust to exceed the overall 20 working day deadline.
- The charge limit is currently £450, calculated at 18 hours work at a flat rate of £25 per hour, as set by government statute. If the estimated cost of complying with the request does not exceed this amount the trust is not entitled to make a charge for fulfilling the request.
- A designated member of staff will be responsible for ensuring requests are fulfilled within the stipulated deadline and recording details of the request on the trust's tracking database.
- Persons requesting data will be supplied with a copy of our complaints procedure upon request. Any complaints regarding Freedom of Information requests must firstly be addressed by the trust. If, once we have had opportunity to reconsider our decision, we believe the initial response was correct the applicant shall be entitled to take the matter to the Information Commissioner's Office and, ultimately, to an Information Tribunal.
- Copies of data supplied will be retained for two years from the date it was put into the public domain.

5.3.6 Applying Exemptions

- A full list of exemptions can be found at the Information Commissioner's website. There are two types of exemption – absolute and qualified. In practice there are very few which are likely to be applied by the education sector.
- The decision to apply absolute exemptions will not be taken by individual members of staff but by a constituted group of at least three of the following: Chair of trustees, other trustees, CEO, Head teacher.
- Even if the group decides information should not be disclosed, a public interest test will be carried out when applying qualified exemptions, to decide whether the public interest in disclosure outweighs the objection to disclosure. If it does the information must be disclosed.
- Advice will be sought from Walsall Metropolitan Borough Council's Information Governance Team or Legal Services if there is any doubt as to whether information should be disclosed.

5.3.7 Logging Requests Received

- The trust will keep a record of all requests received for monitoring purposes, noting:

- a) the date the request was received,
- b) name and contact details of the person or organisation making the request,
- c) the date the request was fulfilled or refused,
- d) the reason for any exemption being applied,
- e) the reason for any failure to meet the 20 day deadline.

5.4 Subject Access Requests

All individuals whose data is held by us, have a legal right to request access to such data or information about what is held. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The headteacher of the child's school should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or legal guardian shall make the decision on behalf of the child. The trust is aware that in some cases it might not be appropriate to release the child's information to the parents. The safety and wellbeing of the child will be the key determining factor in whether or not information can be disclosed.

The GDPR allows exemptions as to the provision of some information, therefore all information will be reviewed prior to disclosure.

No charge will be applied to process the request.

To support subject access requests under the GDPR, requests:

- Should be in writing and be legible in order to correctly identify the requester.
- Must be specific with regards to records or data being requested in order to avoid excessive requests
- must follow the process of confirming identification
- must be made by the data subject or someone authorised to act on their behalf and
- can be sent to/received by any part of the trust

Although we accept requests can be given verbally or via other mediums we will request that you please use and complete our form at [The Forge Brook Trust](#) to support this process and comply with the need to identify the requester and the data being requested.

To be valid under the GDPR requests **do not:**

- have to be submitted on a specific form
- need to mention the GDPR or the term 'subject access'

5.4.1 Confirming Identity

The trust will take reasonable steps to confirm the identity of the requester. However the trust will not make this identification process unnecessarily onerous and in cases where the requester is already known to the trust (e.g. an existing member of staff, a known parent) formal identification will not be sought.

5.4.2 Timing of Requests

All requests will be responded to as promptly as possible, and in any event a response must be provided by no later than 1 month from the day of receipt, however the 1 month time limit will not commence until clarification of information and or identification is sought. Where the case is considered to be complex, the deadline can be extended to 60 days. The requestor should be kept informed of any delays.

5.4.3 Access to Personal Data by an Authorised/ Legal Agent

When an agent makes a request on behalf of a Data Subject, signed authorisation from the Data Subject will be required. The trust may still check directly with the Data Subject whether he or she is happy with the agent receiving the personal data and should highlight the implications of the request.

Any request received from an agent must be accompanied by signed Form of Authority [permission] from the Data Subject. No proof of identity for a Data Subject is required when the application comes from a professionally recognised agent such as Solicitor.

5.4.4 Information Containing Third Party Data

The trust may refuse a subject access request where releasing that information would also involve disclosing information about another individual, except in cases where:

- That individual has consented to disclosure; or
- It is reasonable in all the circumstances to comply with the request without that individual's consent.

The trust will seek to balance the rights of the requestor with the rights of the third party and only release information if, in all circumstances, it is reasonable to do so.

5.4.5 Refusing a Request

Forge Brook Trust uses the presumption of release as the starting point for all valid subject access requests. Where there is a legitimate reason why information should not be disclosed (e.g. the prevention or detection of crime) the applicant will be informed of the reasons why (except in circumstances where disclosure may prejudice the purpose of the exemption applied) and of their right to appeal.

5.4.6 Amendments to Inaccurate Records

The trust acknowledges individual's right to challenge the accuracy of the personal data held about them where they believe it to be inaccurate or misleading. Where information is found to be factually inaccurate it will be updated immediately, where there is dispute between the trust and the data subject as to the accuracy of information, a note will be made on the record to that effect and both sets of information will be kept on the file.

5.4.7 Objections to Processing

Individuals have the right to request that the processing of information about them be restricted or ceased if they believe the information to be inaccurate or being held unnecessarily. The trust

must investigate any such request and rectify if necessary. The Data Subject should be informed before any restriction is lifted.

5.4.8 Releasing personal information to prevent or detect crime

It is trust policy to cooperate wherever possible with requests for personal information for the prevention or detection of crime or identification or apprehension of suspects, but only after satisfactory checks have been completed to protect the rights of Data Subjects. Information will only be released where disclosure meets the criteria outlined in the GDPR

Requests will only be considered from an agency with a crime or law enforcement function, including the Police, HMRC, The UK Border Agency, or the Benefit Fraud sections of DWP or other Local Authorities.

Requests must be in writing and be clear on what is being asked for and why the release of the information is critical to the investigation.

Only information directly relevant to the purpose stated will be released, and only the minimal possible to enable the law enforcement agency to do their job. The transfer of information will be via a secure channel (e.g. secure email or special delivery post).

5.4.9 Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the trust's complaint procedure [FBT Complaints Policy](#)

Complaints which are not appropriate to be dealt with through the trust's complaint procedure can be dealt with by the trusts Data Protection Officer. Should you be dissatisfied with the response you receive from the trusts Data Protection Officer, you can contact the Information Commissioner's Office (ICO) with the details given below:

ICO

Address

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Email Address

Use the online form via this link <https://ico.org.uk/global/contact-us/email/>

Telephone Numbers

Calling from within the UK 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate.

Calling from outside the UK +44 1625 545 745

Part 6: Records Management Policy

6.1 Statement of Intent

1 Functions of Forge Brook Trust

Forge Brook Trust is committed to maintaining the confidentiality of its information and ensuring that all records within the trust are only accessible to the appropriate individuals. In line with the requirements of the 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 intended.

The trust has created this policy to outline how records are stored, accessed, monitored, retained and disposed of to meet the trusts statutory requirements.

This document complies with the requirements set out in the GDPR and Data Protection Act 2018.

2 Purpose of Disposal Schedule

This disposal schedule identifies the disposal arrangements for all manual and electronic records created by Forge Brook Trust. The Schedule complies with the guidelines given under the Information Management Toolkit for Trusts (IRMS). It is advised trusts adapt this template and it be approved by internal management/governors specifically in relation to records disposal.

Approval Date	Approved by	Review Date

Section 6.2 – Operation of this Records Disposal Schedule

1. Closing a file

Manual records should be closed as soon as they cease to be of active use other than for reference purposes. When a file is due to be closed an appropriate member of staff should consult the disposal schedule and mark the front cover of the file, indicating the date on which the file can be destroyed, or whether it should be reviewed by a member of staff. Closing a file simply means that no further papers can be added but the file can be used for reference.

2. Minimum Retention Period

With the exception of pupil files, the minimum retention period required for each type of record is calculated from the point the file/record is closed.

3. Destroy

Where the disposal action states 'Destroy' the records should be kept for the period stated and then destroyed securely. A record must be maintained of the files that have been destroyed.

4. Commitment to preserving files/records

Forge Brook Trust declares that it will take measures to ensure that the records it creates (including electronic records) will be well maintained and protected while they are in its custody.

5. Roles and Responsibilities

The Trust Board is responsible for ensuring that the Trust complies with the commitment laid out in this Policy. The CEO is charged with operational compliance and will assign any specific staff responsibilities as required in order to help fulfil the Trust's commitment to effective records management. **All members of staff** are responsible for creating and maintaining records in accordance with good records management practice.

(Primary trusts only) The trust will not keep any copies of information stored within pupil's records, unless there is ongoing legal action at the time during which the pupil leaves the trust. The responsibility for these records will then transfer to the next trust that the pupil attends.

(Secondary trusts and sixth-form colleges only) If any pupil attends the trust until statutory trust leaving age, the trust will keep the pupil's records until the pupil reaches the age of 25 years.

Section 6.3 – Definitions of Records held by Forge Brook Trust in respect of its Functional Areas.

There are six main functional areas for which Forge Brook Trust keeps records as follows:

1. Management and Organisation
2. Legislation & Guidance
3. Pupils
4. Staff
5. Finance
6. Health & Safety
7. Other

The records contained within these functional areas provide evidence and information about its business activities and are important for the efficient operation of the trust.

1. Management and Organisation

This category comprises records held which relate to the management and organisation of the trust. Typical records would include the minutes of the Trust Board, Local Governing Bodies, the Senior Management Team and Parent/Teachers Association meetings which record the major decision making processes of the trust. Also included are records detailing development, planning and curriculum policies as well as those that demonstrate how the trust reports to its parents and other organisations. Records include the Trust and School Development Plans, the Trust Prospectus, Curriculum policies, Annual Report, Emergency Planning and Business Continuity Plan along with the records of meetings, minutes, and policies documenting the decisions and actions taken within this business function.

2. Legislation and Guidance from DE, ELBs, ESA, & CCMS

Files maintained under this heading contain papers relating to legislation e.g. the Education Act 2011, Circulars, Guidance, Bulletins from the Dept of Education and Education & Library Boards,

CCMS etc, correspondence in connection with Statistical Returns and documents relating to Dept of Education Inspections and Reports.

3. Pupils

Pupil Files contain vitally important records which, not only capture the progress of the student throughout their time at the trust, but also contain personal details and information beneficial to their well being within the trust environment. Such records would include admission data, attendance of the pupils at the trust, timetables and class groupings, education/progress reports of pupils, special education needs documentation, child protection information, disciplinary action taken, examination results, careers advice, trust trip details and medical records (details of medical conditions where medicines are required to be administered at trust).

4. Staff

Staff category refers to those records required for the Human Resources Management function within the trust. These include staff personnel records (recruitment, interview notes, appointments, training, staff development etc), staff salary records, staff induction, sickness records, staff performance review, substitute teacher records and student teachers on teaching practice etc.

5. Finance

This business function maintains records for a range of financial activities such as annual budgets, budget monitoring, Annual Statement of Accounts, procurement, tender information and prices, reconciliation of invoices, audit reports etc.

6. Health & Safety

The health and safety of children and staff is of paramount importance in the trust and such records to support this are kept e.g. Accident/Incident Book, legal/accident/incident forms, risk assessments, fire procedure, CCTV, security system files, health and safety policy statement.

7. Other Retention Records

The table outlines the trust's retention periods for any records held by the trust and the action that will be taken after the retention period, in line with any requirements.

Section 6.4 – Electronic Records

The legal obligation to properly manage records, including compliance with Data Protection legislation, applies equally to electronic records. The main considerations for the management of electronic records are therefore the same as those for manual records. They include:

- Staff must be able to use and access electronic information effectively
- Adequate measures must be in place to ensure all information is stored securely and only available to authorised persons.
- A trust must be able to demonstrate a record's authenticity by ensuring information cannot be altered when declared a record.
- A system must be in place for disposing of electronic records in line with policy once they are no longer needed.

In addition to the above, sufficient backup/recovery processes must be in place. There must also be a process through which links are created from electronic records to any associated manual records. This is to ensure a full record can be considered when necessary i.e. when decision making, providing access or considering a record for disposal.

The Trust Board is ultimately responsible for records management within the Trust. The decision to move towards electronic records must be taken carefully and the Trust Board must satisfy itself that the measures identified above can be achieved. Further information and advice on electronic records can be obtained from the Information and Records Management Society (IRMS). A number of International Standards have also been established to help organisations follow best practice when implementing an electronic records strategy. They include:

ISO 15801:2009 - record authenticity and legal admissibility

ISO 27001 - information security management

BS 10008 - legal admissibility of electronic information standards

SECTION 6.5 – Trust Disposal Schedule

1. Management & Organisation (Trust Board and Senior Leadership Team)

Ref	Record	Minimum Retention Period	Action After Retention
1.1	Trust Board and Local Governing Body Meetings Minutes (master)	Permanent	Consult local archives before disposal
1.2	Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of meeting plus three years	Reviewed annually and securely disposed of, if not needed
1.3	Action plans created and administered by the governing board	Until superseded or whilst relevant	Securely disposed of
1.4	Policy documents created and administered by the trust board	Until superseded or whilst relevant	Securely disposed of
1.5	Records relating to complaints dealt with by the local governing body or headteacher	Current academic year, plus six years If negligence is involved, records are retained for the current academic year, plus 15 years If child protection issues are involved, the records are retained for the current academic year, plus 40 years	Reviewed for further retention in case of contentious disputes, then securely disposed of
1.6	Annual reports required by the DfE	Date of report, plus 10 years	Securely disposed of
1.7	Proposals concerning changing the status of the schools or trust	Date proposal accepted or declined, plus three years	Securely disposed of
1.8	Records relating to the appointment of co-opted trustees or governors	Date of election, plus six months	Securely disposed of

1.9	Records relating to the election of the chair of the trust board or local governing body and the vice chair	Destroyed after the decision has been recorded in the minutes	Securely disposed of
1.10	Meeting schedule	Current academic year	Standard disposal
1.11	Register of attendance at trust board or local governing body meetings	Date of last meeting in the book, plus six years	Securely disposed of
1.12	Records relating to governor monitoring visits	Date of visit, plus three years	Securely disposed of
1.13	All records relating to the conversion of the trust to academy status	Permanent	Consult local archives before disposal
1.14	Correspondence sent and received by the trust board, local governing body or headteacher	Current academic year, plus three years	Securely disposed of
1.15	Trust board and Local Governing Bodies; Records relating to the terms of office of serving trustees/governors, including evidence of appointment Records relating to trustee/governor declaration against disqualification criteria Register of business interests	Date of which the trustees/governors appointment ends, plus six years	Securely disposed of
1.16	Governance code of conduct	Dynamic document – kept permanently	Securely disposed of
1.17	Trustee/Governor training; Records relating to the training required and received by trustees/governors Records relating to the induction programme of new trustees/governors	Date the trustee/governor steps down, plus six years Date on which the governors appointment ends, plus six years	Securely disposed of Securely disposed of

1.18	Governor personnel files	Date on which the trustees/governors appointment ends, plus six years	Securely disposed of
1.19	Log books of activity in the school maintained by the headteacher	Date of last entry, plus a minimum of six years	Reviewed and offered to the local archives if appropriate
1.20	SLT minutes and reports	Date of the meeting/report, plus three years	Reviewed annually and securely disposed of if not needed
1.21	Records created by headteacher, deputy head, heads of year and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed annually and securely disposed of if not needed
1.22	Correspondence created by headteacher, deputy head, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Securely disposed of
1.23	Trust and school development plans	Duration of the plan, plus three years	Securely disposed of

2. Legislation and Guidance from DE, ELB, ESA, CCMS etc

Ref	Record	Minimum Retention Period	Action After Retention
2.1	Correspondence re: Statistical Returns to DE, ELB etc	Current financial year + 6 years	Destroy
2.2	DE Reports, Inspections	Until superseded	Destroy

3. Pupils Records

Ref	Record	Minimum Retention Period	Action After Retention
3.1	Admissions		
3.1a	Register of admissions	Every entry in the register will be preserved for a period of three years after the date on which the entry was made	Review, trusts may wish to keep permanently
3.1b	Successful admissions	Date of admission, plus one year	Securely disposed of

3.1c	Admissions appeal (where the appeal is unsuccessful)	Resolution of the case, plus one year	Securely disposed of
3.1d	Secondary school admissions	Whilst pupil remains at the school, plus one year	Securely disposed of
3.2	Pupil files		
3.2a	Primary schools – pupil educational records	Whilst pupil remains at the trust	Transferred to the next destination – If this is an independent school, home trusting or outside of the UK, the file will be kept by the LA and retained for the statutory period
3.2b	Secondary school and sixth forms – pupil educational records	25 years after pupils date of birth	Review and securely disposed of if no longer needed
3.3	Examination Results		
3.3a	Public examination results	Added to pupil record	All uncollected certificates should be returned to the examination board after reasonable attempts to contact the pupil have failed
3.3b	Internal examination results	Added to pupil record	Transferred to the next school where applicable
3.3c	Examination results trusts copy	Current year, plus six years	Secure disposal
3.3d	SAT's results	25 years after the pupils date of birth	Secure disposal
3.3e	Examination papers	Until the appeals/validation process has been completed	Secure disposal
3.4	Child protection information held on pupil file	Stored in a sealed envelope and placed in the pupils file, retained for the same period as the pupil file	Securely disposed of – shredded

		Records also subject to any instruction given by the Independent Inquiry into Child Sex Abuse (IICSA)	
3.5	Child Protection information held in a separate file	25 years after the pupils date of birth Records also subject to any instruction given by the Independent Inquiry into Child Sex Abuse (IICSA)	Securely disposed of - shredded
3.6	Timetable and Class Groupings (scheme of works, timetable, class record books, mark books, record of homework set, pupils work)	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
3.7	Curriculum returns	Current year, plus three years	Secure disposal
3.8	Attendance		
3.8a	Attendance register	Every entry is retained for a period of 3 years after the date on which the entry was made	Secure disposal
3.8b	Correspondence relating to any absence (authorised or unauthorised)	Current academic year, plus two years	Secure disposal
3.9	SEND files, reviews and EHC plans, including advice and information provided to parents regarding educational needs and accessibility strategy	The pupils date of birth, plus 31 years	Secure disposal

3.10	Self-evaluation forms – Internal moderation	Current academic year, plus one year	Secure disposal
3.11	Self - evaluation forms – External moderation	Retained until superseded	Secure disposal
3.12	Pupils work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Secure disposal
3.13	Extra curriculum activities		
3.13a	Field file – information taken on trust trips	Until the conclusion of the trip, plus one month Where a minor incident occurs, field files are added to the core system as appropriate	Secure disposal
3.13b	Financial information relating to school trips	Whilst the pupil remains at trust, plus one year	Secure disposal
3.13c	Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip	Secure disposal
3.13d	Parental consent forms for school trips where a major incident occurred	25 years after the pupils date of birth on the pupils record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Secure disposal
3.14	Catering and free school meals administration		

3.14a	Free school meals registers (where the register id used as a basis for funding)	Current year, plus 6 years	Secure disposal
3.14b	Meal administration	Current year, plus 3 years	Secure disposal

4. Staff Records

Ref	Record	Minimum Retention Period	Action After Retention
4.1	Operational		
4.1a	Staff members personnel files	Termination of employment, plus six years, unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file will be retained until the IICSA enquiries are complete	Secure disposal
4.1b	Annual appraisal and assessment records	Current academic year, plus six years	Secure disposal
4.1c	Sickness absence monitoring (where sickness pay is not paid)	Current academic year, plus three years	Secure disposal
4.1d	Sickness absence monitoring (where sickness pay is paid)	Current academic year, plus six years	Secure disposal
4.1e	Staff training (where training leads to CPD)	Length of time required by the CPD professional body)	Secure disposal
4.1f	Staff training (except where the training relates to dealing with pupils, e.g. First aid or H&S)	Retain in the personnel file	Secure disposal
4.1g	Staff training (where the training relates to pupils, e.g. safeguarding or other pupil related training)	Date of training, plus forty years	Secure disposal

4.2 Recruitment

4.2a	Interview notes and recruitment records relating to the appointment of a new Headteacher (unsuccessful attempts)	Date of appointment, plus six months	Secure disposal
4.2b	Interview notes and recruitment records relating to the appointment of a new Headteacher (successful appointments)	Added to personnel file and retained until the end of appointment, plus six years, except in cases of negligence or claims of child abuse, then records are retained for at least fifteen years	Secure disposal
4.2c	Interview notes and recruitment records relating to the appointment of new members of staff or governors (unsuccessful candidates)	Date of appointment of the successful candidate, plus six months	Secure disposal
4.2d	Pre-employment vetting information (successful candidates)	For the duration of the employee's employment, plus six years	Secure disposal
4.2c	Proof of identity collected as part of the enhanced DBS check	Where necessary to keep a copy, it will be placed in the staff members personnel file	Secure disposal
4.2d	Evidence of right to work in the UK	Added to the staff personnel file or, if kept separately, termination of employment, plus no longer than two years	Secure disposal
4.3	Disciplinary and grievance procedures		
4.3a	Child protection allegations, including where the allegation is unproven	<p>Added to staff personnel file, and until the individuals normal retirement age, or ten years from the date of the allegation – whichever is longer</p> <p>If allegations are malicious, they are removed from the personal files</p>	Reviewed and securely disposed of

		If the allegations are found, they are kept on the personnel file and a copy provided to the person concerned unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file is retained until IICSA enquiries are complete	
4.3b	Oral warning	Date of warning, plus six months	Securely disposed of, if placed on staff personnel file, to be removed from the file
4.3c	Written warning - level 1	Date of warning, plus six months	Securely disposed of, if placed on staff personnel file, to be removed from the file
4.3d	Written warning - level 2	Date of warning, plus twelve months	Securely disposed of, if placed on staff personnel file, to be removed from the file
4.3e	Final warning	Date of warning, plus eighteen months	Securely disposed of, if placed on staff personnel file, to be removed from the file
4.3f	Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related, then it is disposed of as per 4.3a	Secure disposal

5. Finance records

Ref	Record	Minimum Retention Period	Action After Retention
5.1	Financial records	Current year, plus six years	Secure disposal

5.2	All records relating to the creation and management of budgets, including the annual budget statement and background papers	Life of the budget, plus three years	Secure disposal
5.3	Staff finance records	Current academic year, plus six years	Secure disposal
5.4	Personal bank details	Until superseded, plus three years	Secure disposal
5.5	Contract Management		
5.5a	All records relating to the management of contracts under seal	Last payment on the contract, twelve years	Secure disposal
5.5b	All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Secure disposal
5.5c	Records relating to the monitoring of contracts	Life of the contract, plus six years or twelve years	Secure disposal

6. Health and Safety Records

Ref	Record	Minimum Retention Period	Action After Retention
6.1	Health & safety policy statement	Duration of the policy, plus three years	Secure disposal
6.2	Health & safety risk assessments	Duration of risk assessment, plus three years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	Secure disposal
6.3	Records relating to any reportable death, injury, disease or dangerous occurrence under RIDDOR	Date of incident, plus three years providing that all records relating to the incident are held on the personnel file	Secure disposal
6.4	Accident reporting – adults	Three years after the last entry in the accident book	Secure disposal
6.5	Accident reporting – pupils	Three years after the last entry in the accident book	Secure disposal
6.6	Records kept under the Control of Substances Hazardous to Health Regulations	Date of incident, plus 40 years	Secure disposal
6.7	Information relating to areas where employees and persons are likely to come into contact with	Date of last action, plus forty years	Secure disposal

	asbestos		
6.8	Information relating to areas where employees and persons are likely to come into contact with radiation (maintenance records or controls, safety features and PPE)	Two years from the date on which the examination was made	Secure disposal
6.9	Information relating to areas where employees and persons are likely to come into contact radiation (dose assessment and recording)	Until the person to whom the record relates would have reached seventy-five years old, but in any event for at least thirty years from when the record was made	Secure disposal
6.10	Fire precaution log books	Current academic year, plus three years	Secure disposal
6.11	Health and safety file to show current state of buildings, including all alterations (wiring, plumbing, building works etc.) to be passed on in the case of change of ownership	Permanent	Passed to new owner on sale or transfer of building

7. Retention of Other Trust Records

Ref	Record	Minimum Retention Period	Action After Retention
7.1	Property management		
7.1a	Title deeds of properties belonging to the trust	Permanent	Transferred to new owners if the building is leased or sold
7.1b	Plans of property belonging to the trust	For as long as the building belongs to the trust	Transferred to new owners if the

			building is leased or sold
7.1c	Leases of property leased by or to the trust	Expiry of lease, plus six years	Secure disposal
7.1d	Records relating to the letting of the trust premises	Current financial year, plus six years	Secure disposal
7.2	Maintenance		
7.2a	All records relating to the maintenance of the trust carried out by contractors	For as long as the trust owns the building and then passed onto any new owners if the building is leased or sold	Secure disposal
7.2b	All records relating to the maintenance of the trust carried out by trust employees	For as long as the trust owns the building and then passed onto any new owners if the building is leased or sold	Secure disposal
7.3	Operational administration		
7.3a	General files series	Current academic year, plus five years	Reviewed and securely disposed of
7.3b	Records relating to the creation and publication of the trust brochure and/or prospectus	Current academic year, plus three years	If a copy is not preserved by the trust, standard disposal
7.3c	Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus one year	Standard disposal
7.3d	Newsletters and other items with short operational use	Current academic year, plus one year	One copy archived, other copies standard disposal

7.3e	Visitors books and signing-in sheets	Last entry in the logbook, plus six years	Reviewed then secure disposal
7.3f	Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Current academic year, plus six years	Reviewed then secure disposal
7.3g	Walking bus registers	Date of register, plus six years	Secure disposal
7.3h	Trust privacy notice which is sent to parents	Until superseded, plus six years	Secure disposal
7.3i	Consents relating to school activities	While pupil attends the school	Secure disposal

Part 7: Incident Management Policy

7.1 Policy Statement

Forge Brook Trust processes personal data including special category personal data daily and it is essential that procedures are in place to ensure any threat to the security of that information is minimised and any breaches of the duties in respect of that information are identified and remedied. Any incident that compromises the security of that information, or the ICT system on which it resides, must be managed appropriately and in accordance with legislation and guidance provided by the Information Commissioners Office (ICO).

7.2 Purpose

The purpose of this policy is to ensure that the Trust reacts appropriately to mitigate the risks associated with actual or suspected security incidents relating to personal data. The Trust recognises that there are risks associated with users accessing and handling information to conduct official Trust business.

This policy aims to mitigate the following risks:

- Reduce the impact of personal data breach incidents by ensuring they are followed up correctly
- Improve compliance by ensuring serious incidents are reported to the CEO/Headteacher and the trust Data protection Officer.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

7.3 Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the trust. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Under the UK GDPR, personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This policy applies to all staff employed by our trust, Governors and to external organisations or individuals working on our behalf.

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of personal data. All users have a role to play and a contribution to make to the safe and secure use of personal data and the information that it processes or stores.

You must read, understand and comply with this Policy. This policy sets out what we expect from you in order for the trust to comply with applicable law.

Your compliance with this policy is mandatory. You must also comply with all related Policies and guidelines given. Staff who do not comply with this policy may face disciplinary action.

7.4 Objectives

The main objective of this policy is to ensure security incidents relating to Trust information and ICT systems are reported, recorded and investigated in accordance with the Trust's and legislative standards.

7.5 Legal Requirements

As data controller personal data collected about staff, pupils, parents, governors, visitors and other individuals that is collected and held must be protected from unlawful misuse, loss, theft, accidental disclosure, destruction, corruption or alternation in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) as is currently set out in the Data Protection Bill.

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

7.6 Compliance

If any user is found to have breached this policy, they may be subject to the Trust's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Non-compliance with this policy could have a significant effect on the efficient operation of the Trust and may result in significant financial loss.

The UK General Data Protection Regulation (GDPR) introduces a duty for us to report personal data breaches which are significant to the Information Commissioner. This must be done within 72 hours of the breach, where feasible.

If the breach is expected to adversely impact (or has a high likelihood of impacting) individual's rights and freedoms, we must also inform those individuals 'without undue delay'.

We will keep a record of any personal data breaches, regardless of whether we are required to notify.

7.7 Definition

A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Examples of the most common personal data breaches and information security incidents are listed below. It should be noted that this list is not exhaustive.

- Giving information to someone who should not have access to it – this could be verbally, in writing or electronically.
- Theft / loss of a confidential paper
- Sending personal data to an incorrect recipient .e.g. groups of recipients such as ‘all staff’ by mistake.
- Sending a text message containing personal data to all parents by mistake.
- Printing or copying confidential information and not storing it correctly or confidentially.
- A non-anonymised dataset being published on the trust website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- Computer infected by a Virus or other malware.
- Finding data that has been changed by an unauthorised person.
- Use of unapproved or unlicensed software on Trust ICT equipment.
- Accessing a computer database using someone else’s authorisation (e.g. someone else’s user ID and password).
- Changes to information or data or system hardware, firmware, or software characteristics without the Trust’s knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person

7.8 Procedure for Personal Data Breach Incident Handling

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact The Trust Data Protection Lead who is the person designated as the key point of contact for Personal Data Breaches. You should preserve all evidence relating to the potential Personal Data Breach.

On finding or causing a breach, or potential breach, The Trust Data Protection Lead must immediately notify the Headteacher and Data Protection Officer and take immediate remedial steps to mitigate and remedy the breach that has occurred. All reasonable steps must be taken to retrieve any information that has been unlawfully disclosed. The DPO will provide advice to the trust on the immediate steps to be taken, investigate the report, and determine whether a breach has occurred. The Head teacher will notify the chair of governors if not already notified.

The DPO will assist The Data Protection Lead and relevant staff members or data processors where necessary to mitigate risk and impact.

The actions to be taken will be relevant to specific data types. The actions to minimise the impact of data breaches are set out below. These must, where relevant, be taken to mitigate the impact of different types of data breach. Breaches involving particularly risky or sensitive information must be acted upon swiftly and steps followed through. The effectiveness of these actions will be reviewed and amended as necessary after any data breach.

Example:

If sensitive information has been disclosed via email (including safeguarding records) or other special category data (sensitive information) such as health information is accidentally made available via

email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. Where this is unsuccessful or not possible immediate steps should be taken to contact the recipient with instructions to them to delete the email.

If the sender is unavailable or cannot recall the email for any reason, the Trust Data Protection Lead will ask the ICT department to recall it.

Where members of staff receive personal data sent in error they must alert the sender and Trust Data Protection Lead as soon as they become aware of the error.

In any case where the recall is unsuccessful, The Trust Data Protection Lead will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way. The Trust Data Protection Lead will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The Trust Data Protection Lead will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

7.9 Investigation and Report

The DPO will carry out an internet search to check that the information has not been made public, if it has; we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of Confidentiality
- Any other significant economic or social disadvantage to the individual (s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO within 72 hours of the personal data breach coming to the attention of The Trust Data Protection Lead.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

7.10 Report

The Trust Data Protection Lead will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- o Facts and cause
- o Effects
- o Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored securely in the Forge Brook Trust Offices.

7.11 Review and Planning

Upon the occurrence of a serious breach the DPO and CEO/Headteacher will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible. A report of data protection breaches will be presented to the Trust Board.

Incident Management Flow

Incident Reporter Actions

Head Teacher Actions

DPO Traded Service Actions

