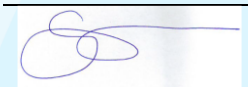
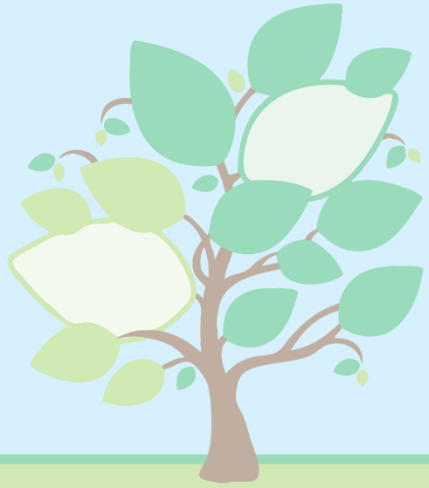
Forest Way School

UK General Data Protection/Security, GDPR, Records Management/ Retention/Information Security & Online Safety Policy

Name:	GAIL SEATON
Signature:	
Title:	HEAD
Date:	MAY 2024
Next Review Date:	MAY 2025



[X] Statutory [ ] Non-Statutory

About This Policy

Forest Way School Data Protection Policy

Forest Way School is committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data and we take that very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

Forest Way School will be responsible for the day-to-day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

Forest Way School is responsible for data held centrally about individuals.

Where we use the phrase ‘we’ that refers to Forest Way School.

What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the Eu on 31 December 2020.

The UK GDPR and DPA 2018 exist to look after individuals’ data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As ‘Public Bodies’ schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and provisions in the Data Protection Act 2018.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Data?

Any information that relates to a living person that identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Privacy Notices that explain how data about specific groups or activities is used and stored are also available. These can be obtained from each school and links on the website to UK GDPR compliance.

What are the key principles of the UK GDPR?

Lawfulness, transparency and fairness

Schools must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent we have a form to complete to allow us to process your request. There are some times when you cannot withdraw consent as explained in 'Data Subjects' Rights'.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the individual school.

Retention

A retention policy is in place that governs how long records are held for. The school have adopted the IRMS (Information and Records Management Society) toolkit regarding the retention and safe disposal of records.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. Please see our Online Safety Policy, Staff Laptop Policy and Encrypted Memory Stick Policy, located at the back of this policy.

Who is a 'data subject'?

An individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

These Data Subject's Rights are set out in more detail in the document 'My Rights – A Guide for Data Subjects'.

Subject Access Requests (SAR)

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if the request is complicated or the data cannot be accessed.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information by paper or electronic form.

If you wish to complain about the process, please see our Complaints Policy and later information in this DPA policy.

Who is a 'Data Controller'?

The academy trust is the Data Controller. They have ultimate responsibility for how the school manage data. They delegate this processing to individuals to act on their behalf, to the relevant school staff

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

As the Data Controller, individuals process data on behalf of the school. This can be a member of staff, possibly a trustee, a consultant or temporary employee.

Who is a 'Data Processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected.

Data Controllers must make sure that Data Processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

Forest Way School must have a reason to process the data about an individual. Our Privacy Notices set out how we use data. The UK GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

Data Portability

The UK GDPR requires an organisation that stores data to enable transfer of that data from one organisation to another. In schools/academies, pupil data is transferred using the Common Transfer File (CTF) which is a DfE standard process. This is outside the scope of data portability in the UK GDPR.

Employee data will be shared to enable new starters and leavers to take up new roles as easily as possible.

When new data is provided to school it will then be administered and processed within the terms of the Data Protection 2018 and any other relevant policy.

Breaches & Non Compliance

If there is non compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed.

Protecting data and maintaining Data Subjects' rights is the purpose of this policy and associated procedures.

Data Protection Breach & Non Compliance Guide

Breach Management Guidance

All staff, governors and trustees must be aware of what to do in the event of a DPA / UK GDPR breach. The 'Data Breach Flowchart' outlines the process.

Most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported so that risks to the data subjects are minimized and well managed.

What is a breach?

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

Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems

- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What staff and governors should do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Data Controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

How is the breach managed?

The breach notification form will be completed and the breach registered on the portal.

Advice will be sought from the Data Protection Officer as required. A plan to effectively manage the breach, who to inform and how to proceed will be put in place.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

Actions and changes to procedures, additional training or other measures may be required to be implemented and reviewed.

The breach report will be within 72 hours of becoming aware of the breach to the Information Commissioner if it is serious.
It may not be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

What happens to the people whose data has been breached?

For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used.

Advice may be taken from the ICO about how to manage communication with data subjects if appropriate.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

What happens next?

The impact of a serious breach will need to be assessed. It be necessary to changes some processes and procedures.

Additional training may be required. IT protocols may need to be reviewed.

The school will work with the Data Protection Officer to ensure that any changes are made to protect and secure information and to learn from any breaches.

Consent

Forest Way School, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the UK GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

This will largely be managed in school.

Consent and Renewal

On our website we have ‘Privacy Notices’ that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent, where required, and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On joining the school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection/consent form.

The contact and consent form is reviewed on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available. This is the obligation of each individual to notify the school of changes.

Pupil Consent Procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child as required.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

CCTV policy

Forest Way School uses closed-circuit television (CCTV) in order to protect the safety of students, staff, parents/carers and visitors.
This policy outlines how the school uses CCTV in line with the principles set out within the Surveillance Camera Code of Practice 2021. All personal data obtained is stored in accordance with UK General Data Protection Regulations (UKGDPR) and Data Protection Act 2018.

Purpose

The CCTV recordings may be used for:

- prevention and detection of crimes, in the school and on the premises
- staff disciplinary and associated processes and appeals
- maintaining a safe environment for the whole school community

CCTV system operation

The CCTV system will be operational 24 hours a day, 365 days a year.
The Data Controller is registered with the Information Commissioner's Office.
All recordings will have date and time stamps.

Location of cameras

The cameras are located in places that require monitoring in order to achieve the purpose of the CCTV system.
Appropriate signs are displayed around the school premises within prominent locations that clearly identifies that CCTV recording is in operation.
Signs are located at the staff entrance, and at the building entrance

General access to CCTV footage

It will not be common practice to release CCTV footage unless satisfactory evidence a secure legal basis can be provided. This is authorised within Section 115, Crime and Disorder Act 1998. In appropriate circumstances, the school may allow authorised personnel to view footage where the above purposes are considered.
The school will maintain a record of all disclosures.
All requests for access should made in writing to the Business Manager and be specific to a date and time frame.
Any disclosure will be done in line with UK GDPR and Data Protection.
The school cannot guarantee disclosure of footage when made under a Subject Access Request due to:

- lack of technical resources available in order to blur or redact the footage
- the release of footage would prejudice an ongoing investigation
- other identifiable individuals have not consented

Authorised CCTV system operators

The school has limited staff members, who are fully trained and understand the importance of confidentiality, authorised to access and operate the CCTV system.
The authorised personnel within school/academy are:

- Headteacher – system manager
- Business manager
- Site manager

Storage of footage

Footage will be retained for no longer than necessary to achieve the purposes of the system.
The retention period will be 30 days. At the end of the retention period, the files will be automatically deleted by the system.
Recordings will be downloaded and encrypted, so that the data will be secure, and its integrity maintained, to ensure it can be used as evidence if required.
All recordings must be logged and traceable throughout their life within the system.

CCTV system security

A full Data Privacy Impact Assessment will be completed upon deployment, replacements, development or upgrading of the CCTV system. This is in line with the UK GDPR principle, Privacy by Design, and ensures the aim of the system is reasonable, necessary and proportionate.
The system will be made secure by the following safeguards:

- the system manager will be responsible for overseeing the security of the footage and recorded images, maintenance and training of authorised personnel
- the system will be check for faults each day and serviced on a regular basis
- the footage will be stored securely and encrypted
- the software updates will be installed as soon as possible
- the recorded footage will be password protected
- the equipment will be located in a secured lockable enclosure accessible only to authorised personnel
- adequate cyber security measures will be in place to protect footage from cyber-attacks
- a register of authorised staff is maintained, reviewed and updated when necessary

Covert recording

The school will only 'covert record' when the following criteria are met:

- an assessment concluded that if we had to inform individuals that recording was taking place it would prejudice our objective

- there is reasonable cause to suspect specific criminal activity or actions that could result in a serious breach of staff or volunteer behaviour expectations is taking place
- covert processing is carried out for limited and reasonable period of time and related to specific suspected criminal activity
- if the situation arises where the school adopts 'covert recording', there will be a clear documented procedure which sets out how the decision to record covertly was reached, by whom and the risk of intrusion on individuals

Complaints

Any complaints should be made in writing to the system manager:

- Business Manager
- Email address: forestway@forestway.leics.sch.uk

Review and monitoring

Appropriate changes will be made accordingly in line with changes to legislation.
The headteacher will communicate changes to all authorised staff members.

Data Protection Officer

We have a Data Protection Officer whose role is:-

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- to monitor compliance with the UK GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- To be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the UK GDPR

Our DPO is John Walker whose contact details are:

Address: 6 Delamore Park, Cornwood, Ivybridge, PL21 9QP

Email: info@phplaw.co.uk

Physical Security

As a school we are obliged to have appropriate security measures in place.

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Site Managers are responsible for authorising access to secure areas along with SLT/Business Manager.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

All sites and locations need to have the suitable security and review measures in place.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

Complaints & the Information Commissioner Office (ICO)

The school Complaint Policy deals with complaints about Data Protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

Forest Way School

Staff Laptop Policy

This policy governs all equipment issued to staff by Forest Way School. The equipment is issued subject to the following conditions:

1. The equipment remains the property of Forest Way School at all times and must be returned to the School at the end of the lease agreement or contractual period. The equipment nominated above is the sole responsibility of the named individual.

2. Maintenance of the equipment is the responsibility of the ICT support department. All maintenance issues must be referred to the ICT support department, through the usual channels.

3. From time to time, it will be necessary for the ICT support department to perform software updates and maintenance for which the equipment must be made available in school when requested.

4. All installed software MUST be covered by a valid license agreement held by the school.

5. All software installation MUST be carried out by the ICT support department in accordance with the relevant license agreements.

6. When equipment is to be used to access the internet other than by the school broadband connection users MUST ensure that spyware protection software, anti-virus software and a firewall are installed. Connection to the internet should not be by wireless router, unless the wireless connection signal is fully encrypted and password protected.

7. No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.

8. Protective software must be updated regularly. For laptop computers, it will be necessary to connect them to the school network to update the antivirus software. This should be done regularly with updates continuously added automatically during normal in school use at least twice a weekly.

9. The user of the equipment is responsible for all personal files and data stored on the equipment. In order to facilitate data backups all laptops must be regularly connected to the school network.

10. The ICT support department cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.

11. If school equipment is to be used by anyone other than the member of staff responsible for it that user must have a separate account set up by the ICT Support Department. The laptop must remain in the users possession at all times.

12. Equipment is insured by Forest Way School whilst in school premises or the registered users home. Whilst in transit it is only covered if it is in the possession of the user. If the equipment is in a situation where it is not covered by the School insurance, users are responsible for organising their own insurance.

Name of recipient	
Recipient's Signature	
Date Signed	

Forest Way School

Encrypted Memory Stick Acceptable Use Policy

Forest Way School permits only the use of encrypted memory sticks and other removable storage in all computers (laptops, desktops, servers etc.). The use of unencrypted memory sticks is not permitted*.

Any member of staff who requires the use of a memory stick will be provided with an encrypted memory stick. In order to receive a memory stick, the following form must be signed. By signing this form the member of staff agrees to the following:

- They will provide a strong password which is known only to them. They will not record this password in any shape or form. This password will enable access to the encrypted memory stick.
- They will accept that in the event of their password being forgotten that the data placed on the memory stick is lost forever. It is impossible to circumvent the encryption on the memory sticks provided.
- They will accept that in the event of supplying an incorrect password a number of times** their data will be lost forever.
- They will ensure that they only use their memory stick for data transfer not storage. The latest copy of any file on the memory stick should be placed back onto the school network as soon as possible.
- They will ensure that they do not place sensitive data on a computer outside the school network.
- They will ensure that any computer they use the memory stick in off the premises has up to date antivirus software so as not to infect the school network upon inserting it into a school computer.
- They will never use their memory stick to store copyrighted material or transfer said material to the school network. They will, in the event of loss, pay for a replacement of equivalent size and encryption level themselves.

Name: _____

Location
(e.g. Acorns 1): _____

Signed: _____

Date: _____

DISPLAY SCREEN EQUIPMENT USER
EYE TEST

All employees who are designated as a Display Screen Equipment User has the right to request an eye test.

This must be organised, in consultation with the employee's academy senior manager, through an optician of the employee's choice.

It is the employee's responsibility to make arrangements to have the eye test carried out, and as funding is delegated to the academy they are obliged to refund the cost of an eye test for Display Screen Equipment User.

Following the initial eye test, the frequency of any follow up test will be decided solely by the optician.

Display Screen Equipment Assessment Checklist

This assessment is undertaken in accordance with the Health and Safety (Display Screen Equipment) Regulations 1992 as amended by the Health & Safety (Miscellaneous Amendments) Regulations 2002

User name:	Location:
User occupation:	

Display Screens	Yes	No	Things to consider	Comments
Are the characters clear and readable			Make sure the screen is clean and cleaning materials are made available. Check that text and background colours work well together.	
Is the text size comfortable to read?			Software settings may need adjusting to change text size.	
Is the image stable, ie free of flicker and jitter?			Try using different screen colors to reduce flicker, eg darker background and lighter text. If problems still exist, get the set-up checked, eg by the equipment supplier.	
Is the screen's specification suitable for its intended use?			For example, intensive graphic work or work requiring fine attention to small details may require large display screens.	
Are the brightness and/or contrast adjustable?			Separate adjustment controls are not essential, provided the user can read the screen easily at all times.	
Does the screen swivel and tilt?			Swivel and tilt need not be built in; you can add a swivel and tilt mechanism. However, you may need to replace the screen if: swivel/tilt is absent or unsatisfactory; work is intensive; and/or the user has problems getting the screen to a comfortable position.	
Is the screen free from glare and reflections? Are adjustable window coverings provided and in adequate condition?			Use a mirror placed in front of the screen to check where reflections are coming from. You might need to move the screen or even the desk and/or shield the screen from the source of reflections. Screens that use dark characters on a light background are less prone to glare and reflections. Check that blinds work. Blinds with vertical slats can be more suitable than horizontal ones. If these measures do not work, consider anti-glare screen filters as a last resort and seek specialist help.	
Keyboard	**Yes**	**No**	**Things to consider**	**Comments**
Is the keyboard separate from the screen?			This is a requirement, unless the task makes it impracticable (eg where there is a need to use a laptop).	
Does the keyboard tilt?			Tilt need not be built in.	
Is it possible to find a comfortable keying position?			Try pushing the display screen further back to create more room for the keyboard, hands and wrists. Users of thick, raised keyboards may need a wrist rest.	

Does the user have good keyboard technique?			Training can be used to prevent: hands bent up at wrist; hitting the keys too hard; Overstretching the fingers.	
Are the characters on the keys easily readable?			Keyboards should be kept clean. If characters still can't be read, the keyboard may need modifying or replacing. Use a keyboard with a matt finish to reduce glare and/or reflection	
Mouse, trackball etc	**Yes**	**No**	**Things to consider**	**Comments**
Is the device suitable for the tasks it is used for?			If the user is having problems, try a different device. The mouse and trackball are general-purpose devices suitable for many tasks, and available in a variety of shapes and sizes. Alternative devices such as touch screens may be better for some tasks (but can be worse for others).	
Is the device positioned close to the user?			Most devices are best placed as close as possible, eg right beside the keyboard. Training may be needed to: prevent arm overreaching; tell users not to leave their hand on the device when it is not being used; Encourage a relaxed arm and straight wrist.	
Is there support for the device user's wrist and forearm?			Support can be gained from, for example, the desk surface or arm of a chair. If not, a separate supporting device may help. The user should be able to find a comfortable working position with the device.	
Does the device work smoothly at a speed that suits the user?			See if cleaning is required (eg of mouse ball and rollers). Check the work surface is suitable. A mouse mat may be needed.	
Can the user easily adjust software settings for speed and accuracy of pointer?			Users may need training in how to adjust device settings	
Software	**Yes**	**No**	**Things to consider**	**Comments**
Is the software suitable for the task?			Software should help the user carry out the task, minimise stress and be user-friendly. Check users have had appropriate training in using the software. Software should respond quickly and clearly to user input, with adequate feedback, such as clear help messages.	
Furniture	**Yes**	**No**	**Things to consider**	**Comments**
Is the work surface large enough for all the necessary equipment, papers etc?			Create more room by moving printers, reference materials etc elsewhere. If necessary, consider providing new power and telecoms sockets, so equipment can be moved. There should be some scope for flexible rearrangement.	
Can the user comfortably reach all the equipment and papers they need to use?			Rearrange equipment, papers etc to bring frequently used things within easy reach. A document holder may be needed, positioned to minimize uncomfortable head and eye movements.	
Are surfaces free from glare and reflection?			Consider mats or blotters to reduce reflections and glare.	
Is the chair suitable? Is the chair stable? Does the chair have a working: seat back height and tilt adjustment?			The chair may need repairing or replacing if the user is uncomfortable, or cannot use the adjustment mechanisms.	

seat height adjustment? swivel mechanism? castors or glides?				
Is the chair adjusted correctly?			The user should be able to carry out their work sitting comfortably. Consider training the user in how to adopt suitable postures while working. The arms of chairs can stop the user getting close enough to use the equipment comfortably. Move any obstructions from under the desk.	
Is the small of the back supported by the chair's backrest?			The user should have a straight back, supported by the chair, with relaxed shoulders.	
Are forearms horizontal and eyes at roughly the same height as the top of the screen?			Adjust the chair height to get the user's arms in the right position, then adjust the screen height, if necessary.	
Are feet flat on the floor, without too much pressure from the seat on the backs of the legs?			If not, a foot rest may be needed	
Environment	**Yes**	**No**	**Things to consider**	**Comments**
Is there enough room to change position and vary movement?			Space is needed to move, stretch and fidget. Consider reorganizing the office layout and check for obstructions. Cables should be tidy and not a trip or snag hazard.	
Is the lighting suitable, eg not too bright or too dim to work comfortably?			Users should be able to control light levels, eg by adjusting window blinds or light switches. Consider shading or repositioning light sources or providing local lighting, eg desk lamps (but make sure lights don't cause glare by reflecting off walls or other surfaces).	
Does the air feel comfortable?			SCREENs and other equipment may dry the air. Circulate fresh air if possible. Plants may help. Consider a humidifier if discomfort is severe.	
Are levels of heat comfortable?			Can heating be better controlled? More ventilation or air-conditioning may be required if there is a lot of electronic equipment in the room. Or, can users be moved away from the heat source?	
Are levels of noise comfortable?			Consider moving sources of noise, eg printers, away from the user. If not, consider soundproofing.	

Final questions to users...

Ask if the checklist has covered all the problems they may have working with their computer.

Ask if they have experienced any discomfort or other symptoms which they attribute to

working with their computer.

Ask if the user has been advised of their entitlement to eye and eyesight testing.

Ask if the user takes regular breaks working away from their computer.

Any comments/Recommendations

Person undertaking assessment.....

Position.....

Review by (date)……..

Signed.....…… Date.....

Online Safety

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle

cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees safeguarding, and therefore online safety, is James Shanley.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the SLT in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the SLT, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems at least on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Working with the DSL or their deputies to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour and Discipline Policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL or their deputies to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

The use of technology can bring huge benefits to all pupils at Forest Way School, educationally, socially and to enable them to lead as full a life as possible. It is vital that we educate our pupils to use the technology and online services in a manner that helps to protect them from harm and ensures their safety and wellbeing.

We want our pupils to be able to use technology and online services as safely and independently as they can, in readiness for life beyond school. The school's scheme of work is progressive, building upon previous learning, to allow pupils to learn about Online Safety in a manner that is appropriate to both their level of online usage and their level of understanding.

The strands covered by the Scheme of Work are:

Online relationships	This strand teaches and encourages pupils to be good Digital Citizens. Using online services responsibly and in a way that is kind and beneficial to other users.
Online bullying	This helps to prepare the pupils for the fact that not everything or everyone they encounter in the online world will be kind to them and that sometimes they may encounter people or situations that can upset them. It teaches them how to deal with these situations when they arise and also what to do if they see it happening to somebody else.
Reliability of information	Pupils are taught to understand that not everything they read or see online is true or helpful. They are given strategies to help them decide what information to trust and also the implications of them sharing something that is not true. Pupils are also taught about fraud and learn strategies to help them avoid becoming victims of fraud.
Online reputation	In an age of social media, pupils are taught about the implications of sharing things online and how this may harm them in ways they might not foresee.
Privacy and security	This strand teaches the pupils about the importance of keeping their personal details and access to services private and secure.
Health and wellbeing	At a time when technical devices are almost ubiquitous, pupils are taught about responsible use and the implications to their health and wellbeing if devices are used too often and for too long.

The scheme of work shows progression through an understanding of Online Safety. It contains 6 areas of progression with statements in progressive order for each of the 6 strands of Online Safety, moving towards a high level of understanding that will support the pupils whether they continue to be supported, live independently or move into the world of employment. This scheme of work draws upon the National Curriculum in England, the Education for a Connected World Framework, the Government's "Teaching online safety in schools" guidance as well as guidance from Online Safety charities such at the Safer Internet Centre, The NSPCC and ChildNet.

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or any Deputy DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school will also provide information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour and Discipline Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use Agreements in Appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school but should only use them when given permission to do so.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendix 1).

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure and ensure all use complies with the school's Adult Acceptable Use Policy (see Appendix 2).

The computers, electronic media and services provided by the school are primarily for educational use to assist staff in the performance of their job. Staff, learners, and parents are expected to demonstrate a sense of responsibility and not abuse this privilege.

Any devices provided by the school for the purpose of remote learning belong to the school and must be used under the supervision of an adult in accordance with the Acceptable Use Policy.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Acceptable Use Policy for Pupils and the Behaviour and Discipline Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Attendance, Conduct and Grievance Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Remote Learning

During the national lockdowns during the Covid-19 pandemic, Forest Way, like most schools, stayed open throughout the period to support its most vulnerable pupils and those of key workers. As all students at Forest Way have an EHCP, and are by definition a vulnerable group, this aspiration stays in place. However, during the lockdowns, many pupils are not in school and it is also important to plan for the potential closure of Bubbles or a whole school closure that ensures the minimum disruption to learning and the maintenance of effective safeguarding.

In the case of remote learning, the provisions of this policy must be applied in conjunction with those in the Remote Learning Policy.

12.1 “Live” Lessons and Pre-recorded Video

The school uses Microsoft Teams to provide remote learning for those children not in school both through the sharing of documents and pre-recorded video as well as the use of the virtual meeting functionality to provide “live lessons”. When pre-recording videos or attending “live” lessons or meetings, and in line with the Remote Learning Policy, staff will ensure they adhere to the following:

- Attending “live” virtual meetings or “live” lessons with parents and/or pupils –
    - Staff will be appropriately dressed as per the school’s dress code
    - If TEAMs calls are made from a home setting than the staff members location within the home should be in suitably professional setting with the background blurred.
    - To safeguard both children, staff and parents the TEAMs recording facility should not be used.
    - Within school, the virtual lesson will be conducted in a room with another adult in place.
    - A parent or carer must be present during the live meeting.

12.2 Security of Remote Learning

- Learners have individual usernames and passwords for security.
- Users should not give out their username or passwords to anyone.
- Children and staff must not disclose any password or login name given to anyone or allow anyone else to use a personal account.
- Children and staff must not attempt to gain access to the school network or any internet resource by using somebody else’s account name or password.
- Staff and children must ensure terminals. Laptops or devices are logged off when left unattended.
- Children are only allocated to Teams in which they are grouped in school, e.g. their class and ability group. They are not able to see any other groups.
- Please be aware that all the group members within each Team are able to see comments made, including learners, teachers and parents. A team may have multiple teachers as group members for monitoring and management purposes.

12.3 Reporting of Online Safety incidents during home learning

Any concerns or incidents related to Online Safety that arise during a home learning period must be reported to the Headteacher immediately and will be dealt with in line with the school’s Child Protection Policy. Any material deemed as inappropriate content will be removed at the school’s discretion and will be dealt with in accordance with the school’s Child Protection Policy and Behaviour and Discipline Policy.

13. Monitoring arrangements

The DSL and their deputies log behaviour and safeguarding issues related to online safety in accordance with the schools' Child Protection Policy.

This policy will be reviewed annually by the headteacher. At every review, the policy will be shared with the governing board.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and Discipline Policy
- Staff disciplinary procedures
- Data Protection/Security and GDPR Policy
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Forest Way School Acceptable Use Policy for Pupils

Appendix 2: Forest Way School Adult Acceptable Use Policy


The image part with relationship ID rId9 was not found in the file.

Name _____

Signed _____ Date _____

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Records Management Policy

Introduction and principles

Management of records by a Public Authority is a legal obligation (Section 46 of the Freedom of Information Act 2000).

The Code issued on 15 July 2021 sets out key principles about records and their management. These are the:

- value of the information
- integrity of the information
- accountability for the information

There are a range of statutory, regulatory and guidance that oblige us to accept, create, use, edit, store, and dispose of records. It is necessary to establish clarity about records keeping systems.

Aims

- to effectively manage the records that are created and are integral to the operation of the school
- to confirm a clear framework to manage records and information within the school
- to provide an environment where records are stored securely
- to ensure that records are accessible to those who need them
- to ensure that the school workforce responsible for records management understand these obligations
- to give effect to the s.46 Code of Practice our records management will take note of the principles it sets out

Scope

This policy applies to the school workforce and to all school records, whether the records originate within the school or are shared with the school by other means.

Records that are shared with third parties as a result of consent, regulatory obligations or contractual agreements are within the scope of this policy.

In school, the records that we access and hold originate are stored in a variety of formats, that include physical, digital, electronic audio/visual records. Some are held locally in school, others are hosted by third party providers.

All records are within the scope of this policy, records are required to be stored and retained in accordance with the document retention schedule attached to this policy.

Records may refer to individuals, financial planning tools, contracts, commercial organisations, public authorities, or charitable organisations. Some records will contain personal data. Record retention and storage will be reviewed from time to time to ensure that the aims of this policy are met.

Responsibilities and actions

The governing board is ultimately responsible for this policy, however on a daily basis operational management of the policy is delegated to the headteacher and senior leadership team.

Management of the policy will be reviewed at governing board meetings on at least an annual basis.

The headteacher will be required to monitor compliance with this policy by undertaking at least an annual check to determine if records are stored securely and can be accessed appropriately, in accordance with requirements in this policy.

An active retention policy is applied to confirm what records are to be retained and set out a timeline for their secure disposal.

Individual school staff, contractors and volunteers and employees have personal responsibility for records within their control and day to day handling by ensuring that:

- records are to be handled in accordance with the school polices and good practice for secure storage and usage
- keep accurate records as required
- personal data contained in records is used in compliance with the UK GDPR and school data protection policies and protocols
- personal information is shared appropriately and with a proper legal basis with any third party
- records are securely disposed in accordance with the school's records retention schedule.

Child Abuse Records

The Independent Inquiry into Child Sexual Abuse (Final Report 2022) recommends that any records that relate (or could relate) to sexual abuse should be retained for 75 years or 10 years past the retirement of a relevant member of staff, whichever is the longer term. We shall implement this and ensure that notification of the relevant records is made in the event of any transfer.

Relationship with existing policies and obligations

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- Privacy Notices
- Data Sharing Agreements
- Information Security policy
- IT security and use polices
- Records retention policy/guidelines
- and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school

Appendix 1

The school keeps a wide variety of records that may include (but are not limited to):

Students

- personal information
- parent/carer contact information
- school reports
- behaviour logs
- exam and testing outcomes – internal and external
- child protection information
- allegations of a child protection nature made against a member of staff (including unfounded allegations)
- attendance – attendance registers, authorised absence correspondence
- SEND – reviews, advice to parents/carers, accessibility strategy
- pupil premium/sixth form bursary – evidence of eligibility
- free school meals eligibility
- services and pupil premium eligibility
- LAC status
- medical – individual health plans, first aid records
- biometric records

Management of the school

- governing board records - agendas, minutes, resolutions, reports
- governors personal details
- declarations of interests
- CPD and training
- statutory documents for companies house (if applicable)
- accounts and trust report (if applicable)

- school development plans and school improvement plans
- leadership meetings, minutes and actions
- admission details
- school visitor logs
- health and safety records
- fire risk assessments
- risk assessments
- social media
- newsletters and external communication records

Human Resources

- job descriptions
- application forms
- personnel files for all staff – including personal contact details
- appraisals
- performance reviews
- employment suitability checks
- contracts of employment
- records of disciplinary and grievances process
- allegations and LADO referrals
- referrals to the TRA and/or DBS
- payroll and pensions – maternity/paternity pay, family leave records

Financial Management

- budgets and funding details as required by the funding agreement, academies financial handbook and company law (if applicable)
- risk management and insurance – employer's liability insurance certificate
- asset management records
- asset register
- all necessary financial records
- contracts
- contract management and procurement
- school payment and meals management
- property management
- condition surveys
- hire agreements
- maintenance – log books, warranties and contractor information
- health and safety information

- curriculum & attainment
- teaching and learning planning
- timetabling and resource planning
- prospectus and website
- statistics and evidence of learning outcomes, targets
- pupil work records
- trip and visit records

External Records

- central government and local authority
- local authority – census returns, attendance returns
- central government – returns made to DfE/ESFA
- Ofsted
- referrals to third party agencies
- legal action involving the school
- ICO action
- enquiries and investigations by external bodies

Retention Policy Overview

A comprehensive retention policy is in place. The school subscribe to the Records Management Society and retention and disposal is undertaken following their guidance.

The Data Controller must ensure that a suitable retention policy is in place and is effective. This will be with the support of the DPO/Data Compliance Manager/Records Management Society.

Within Forest Way School responsibility for secure retention and review is as follows

Type of Data	**Responsible Person**
Pupil Progress and Attainment	Headteacher/Business Manager

SIMS or equivalent	Headteacher/Business Manager
Financial	Headteacher/Business Manager
Human Resources	Headteacher/Business Manager
Health and Safety Records	Headteacher/Business Manager
Governance	FGB/Headteacher
Hardware	Headteacher/Business Manager
Software	Headteacher/Business Manager
Statutory and Regulatory	Headteacher/Business Manager
SEN and Health	Headteacher/Business Manager
Safeguarding	Headteacher
Servers	Headteacher/Business Manager/IT
IT to include PCs, laptops and portable storage	Headteacher/Business Manager/IT
Digital records	Headteacher/Business Manager
Emails	Headteacher/Business Manager

Access Control Rules and Rights for Users guidance sets out the level of access across the organisation.

Destruction
At the point of destruction the 'Data Destruction Log' will be completed

Information security policy

Introduction

Information security is everyone's responsibility. Personal and sensitive data is used, stored, shared, edited and deleted each day.
This policy explains staff responsibilities that are already in contracts of employment and reflects statutory obligations.
Details of how personal data is used is contained within privacy notices. The data protection policy sets out how the school's statutory obligations are managed.
The policy applies to all school staff which includes governors, agency staff, contractors, work experience students and volunteers when handling personal data.

Information security breach

Information security breaches can happen in a number of different ways.
Examples include:

- sending a confidential email to the wrong recipient
- letters sent to the wrong address with health and SEN data included

- overheard conversations about a member of staff's health
- an unencrypted laptop stolen after being left in a car
- hacking of school systems
- leaving confidential documents containing personal data in a car that was stolen

These would all need to be reported to the school data compliance officer. Anything which a staff member becomes aware of even if they are not directly involved in needs to be reported. For example, if they know that document storage rooms are sometimes left unlocked at weekends.
The sooner the breach is notified to the right person, the sooner and more effectively it can be managed.
In certain situations, it is necessary to report a breach to the Information Commissioner's Office (ICO), the data protection regulator, and notify those whose information has been compromised within strict timescales. This is another reason why it is vital breaches are reported immediately.

Privacy on a day-to-day basis

Staff must be aware of data protection and privacy whenever they handle personal and sensitive data.

Sensitive personal data

Data protection is about looking after information about individuals. Even something as simple as a person's name or their attendance record is personal data. However, some personal data is more sensitive. This is called **sensitive personal data** in this and the data protection policy. Greater care about how that data is used is required.
Sensitive personal data includes:

- safeguarding and child protection matters
- serious or confidential physical or mental health conditions
- special education needs (SEN) information
- details of serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved
- financial information about parents/carers and staff
- racial or ethnic origin
- political opinion
- religious beliefs or beliefs of a similar nature
- trade union membership
- genetic information
- sexual life or orientation
- actual or alleged criminal activity
- biometric information (e.g. fingerprints used for cashless catering)

Minimising the amount of personal data held

Restricting the amount of personal data, we hold on an individual is needed to help keep the personal data safe. You should never delete personal data unless you are sure you are allowed to do so. If you would like guidance on when to delete certain types of information please speak to the Business Manager.

Basic IT expectations

Lock computer screens: A staff member's computer screen should be locked when it is not in use, even if they are only away from the computer for a short period of time. To lock a computer screen, press the "Windows" key followed by the "L" key.
If staff are not sure how to do this speak to a member of the IT department.
Be familiar with the tech: Staff should make sure that they familiarise themself with any software or hardware that they use. In particular, they need to understand what the software is supposed to be used for and any risks.
For example:

- electronic registers – set to the correct view so students cannot see personal data of classmates
- virtual classrooms – be careful that confidential information is not uploaded for students to access
- shared drives – ensure you know where to store information containing sensitive personal data

Hardware and software not provided by school:
Staff must not use, download, or install any software, app, programme, or service without permission from the IT Department. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to IT systems without permission.
Private cloud storage: Staff must not use private cloud storage or file sharing accounts to store or share school documents.
Portable media devices: The use of portable media devices (such as USB drives) is not allowed unless those devices have been given to staff by the school and staff have received training on how to use those devices securely. The IT Department will protect any portable media device given to you with encryption.
IT equipment: If staff are given IT equipment to use (this includes laptops, printers and phones) staff must make sure that this is recorded on IT equipment asset register. IT equipment must always be returned to the IT Department even if you think that it is broken and will no longer work, and the asset register updated accordingly.

Passwords

Passwords should be long and difficult to guess. Staff should not choose a password which is so complex that it's difficult to remember without writing it down.
Passwords should not be disclosed to anyone else.
Staff should not use a password which other people might guess or know, or be able to find out, such as their address or birthday.
Staff must not use a password which is used for another account. For example, staff must not use a password used for their private email address or online services for any school account.
Passwords (and any other security credential staff are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

Emails

When sending emails staff must take care and check to ensure that the recipients are correct.
Sending an email to multiple recipients, staff must be sure to check that they are using the correct 'To:' 'CC:' or 'BCC:' function.
If the email contains any personal data then staff should ask themselves is this the best communication method. Sometimes it is unavoidable so staff should ensure the email is sufficiently encrypted and ask an authorised staff member to check the email addresses have been entered accurately. When sending personal data over email, staff should consider inputting the information into an attachable document which is password protected.
Staff must not use a private email address for any school related work. A school email address must only be used. This also applied to governors/trustees.

Paper files

Keep under lock and key: Staff must ensure that papers which contain personal data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.
If the papers contain critical personal data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below.
Information held in paper form must not be stored in any other location, for example, child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (DSL) room.

Cabinet	Location	Access
Child protection	DSL's office	Headteacher and DSL's
Financial information	Head's room	Headteacher and authorised personnel e.g. \Business Manager
Health information	Medical room	Headteacher and authorised personnel e.g. Medical Staff

Disposal: Paper records containing personal data should be disposed of securely shredding the material and disposing the paper waste in recycling. Personal data should never be placed in the general waste.
Printing: When printing documents, staff must collect everything from the printer straight away, otherwise there is a risk that confidential information being read or picked up by someone else. If you see anything left by the printer which contains personal data then you must hand it in to the office.
Put papers away: Staff should always keep a tidy desk and put papers away when they are no longer needed.
Post: Staff also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If staff need to send something in the post that is confidential, consider asking the IT team to put it in on an encrypted memory stick or arrange for it to be sent by courier.

Working off-site

Staff might need to take personal data off-site for various reasons such as remote working or supervising a school trip. This does not breach data protection law if the appropriate safeguards are in place to protect personal data.
For school trips, the trip supervisor should decide what information needs to be taken and who will be responsible for looking after it. Any personal data taken off-site must be returned back to school.
When a staff member works from home, they should check with SLT whether any additional arrangements need to be put in place to ensure the security of data.
Only take the minimum: When working away from school staff must only take the minimum amount of information with them. For example, if only eight out of a class of twenty pupils are attending the trip, then the teacher should only take the information about the eight pupils.
Working on the move: Staff must not work on documents containing personal data whilst travelling if there is a risk of unauthorised disclosure. For example, if working on a laptop on a train, the individual should ensure that no one else can see the laptop screen and they should not leave any device unattended where there is a risk of theft.
Paper records: If staff need to take hard copy records with them then they should make sure that they are kept secure.
For example:

- documents should be kept in a locked case
- information should be kept with them at all times
- the individual must keep the documents out of plain sight
- if the individual has a choice between leaving documents in a vehicle and taking them with them (e.g. to a meeting) then they should be taken with them

Public Wi-Fi: Staff must not use public Wi-Fi to connect to the internet. If working in a public café, the individual should use their 4G or 5G.

Breach of this policy

Any breach of this policy will be taken seriously and may result in disciplinary action.
A member of staff who deliberately or recklessly obtains or discloses personal data held by Forest Way School without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.
This policy does not form part of any employee's contract of employment.
We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by email.

Appendix 1 - Protocols for the use of phone in school

Responsibility

Mobile phones brought into school are entirely at the staff member, pupil's, parent's or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any mobile phone.
The school reserves the right to search the content of any mobile phone on the school premises where there is reasonable suspicion that it may contain undesirable

material, including those which promote pornography, violence or bullying. Staff mobiles may be searched at any time as part of routine monitoring.
The recording, taking and sharing of images, video and audio on any mobile phone is prohibited; except where it has been explicitly agreed otherwise by the headteacher.
All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

Mobile phones are not permitted to be used in certain areas within the school/academy premises, e.g. changing rooms and toilets.

Staff

All staff mobile phones must be secured in locked areas
Staff members may use their phones during school break times in certain areas.
Mobile phones will not be used in any way during lessons or formal school time.
They should be switched off or silent at all times.

Staff use of mobile phones

Staff are not permitted to use their own mobile phones for contacting pupils, parents/carers or their families within or outside of the setting in a professional capacity.
Staff will be issued with a school/academy phone where contact with pupils, parents or carers is required.
Staff will also be issued with a school phone whilst on educational off-site visits.
Alternatively, staff may have permission from the headteacher or the trip supervisor to bring their own mobile phones on trips to be used strictly for communication with the school or for emergency situations.
Bluetooth communication should be 'hidden' or switched off. They will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
If members of staff have an educational reason to allow pupils to use mobile phones or as part of an educational activity, then it will only take place when approved by the senior leadership team.
Staff must not use their personal mobile phone to take photos or videos of pupils and will only use work-provided equipment for this purpose.
If a member of staff breaches the school policy then disciplinary action may be taken.
Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school owned device, they should use their own device and hide their own mobile number for confidentiality purposes.

Visitors

All visitors are requested not to use their phones on the school premises and to keep their phones on silent.

Parents and pupils

Where parents or pupils need to contact each other during the school day, they should do so through the school's telephone.

Pupils' use of personal devices

The school strongly advises that pupil mobile phones should not be brought into school.
The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
If a pupil breaches the school policy then the phone will be confiscated and will be held in a securely in the school office until the end of the day
Mobile phones are prohibited to be taken into any examination. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the schoolday, but to contact the school office.

Digital images and videos

In Forest Way School:

- consent is sought from parents/carers for use of images and videos involving their child as part of the Consent Formsb when their son/daughter joins the school
- pupils are not identified in online photographic materials or include the full names of the pupil
- staff confirm that they have read and understood this policy
- any photos used on the school website or prospectus, parents/carers will be asked to provide consent
- pupils are taught about how images can be manipulated in their e-safety education programme
- pupils are advised to be very careful about placing any personal photos on any 'social' online network space
- pupils are taught that they should not post images or videos of others without their permissions