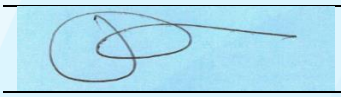
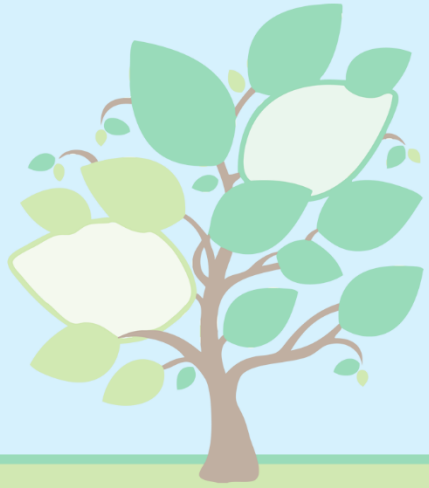
Forest Way School

Data Protection/Security, GDPR & Online Safety Policy

Name:	GAIL SEATON
Signature:	
Title:	HEAD
Date:	February 2022
Next Review Date:	February 2023



[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

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 schools and trust central team manage data. They delegate this processing to individuals to act on their behalf, that is the trust central team and the relevant school staff in each setting.

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

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. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the Local Authority.

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.

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.

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

We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:-

- Detection and prevention of crime
- School staff disciplinary procedures
- Pupil behaviour and exclusion management processes
- To assist the school in complying with legal and regulatory obligations

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:
Office 7, The Courtyard
Gaulby Lane,
Stoughton
LE2 2FL

Email info@jawalker.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? seat height adjustment? swivel mechanism? castors or glides?			The chair may need repairing or replacing if the user is uncomfortable, or cannot use the adjustment mechanisms.	
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.

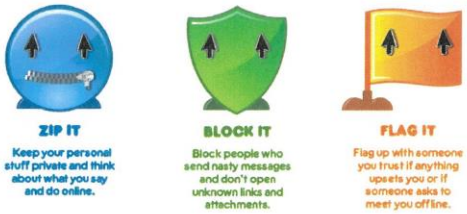
14. Links with other policies

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

Forest Way School
Acceptable Use Policy for Pupils



To keep me safe whenever I use the internet or email, I promise…

- to keep my username and password private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer equipment in school…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will only use my mobile phone and other handheld devices when given permission to do so
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites whilst at school
- I will only access my school email whilst at school
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website
- I will only print with permission from an adult

If I break these rules…

- I understand that the school's behaviour guidelines will be followed
- I understand that Police could be involved if something I did was illegal

I have read and understand this policy and agree to follow it.

Name of pupil _____

Signed _____ Date _____

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the internet.

Parent/Carer signature _____ Date _____

19

Appendix 2: Forest Way School Adult Acceptable Use Policy

Forest Way School
Adult Acceptable Use Policy

This policy governs acceptable use for all adults accessing the Forest Way School network, this includes all staff, governors, volunteers and any other adults given access to the system.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work. However it is important to recognise the dangers to both adults and young people when using digital technologies.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies including personal mobile devices.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also applies to the use of school ICT systems out of school (eg laptops, email, VLE etc) and remote access.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.
- Visitors will be logged in by the network manager/IT technician using a visitor login.
- I will not name my place of work on social networking sites such as Facebook.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify pupils by name, or other personal information.
- I will only use chat and social networking sites in school in accordance with school policy.
- I will only communicate with pupils and parents /carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to

technologies:

- All Forest Way School data should only be stored on the Forest Way School Network or encrypted devices provided by school.
- Forest Way School does not allow the use of Cloud storage for users of its network. (Forest Way does utilise Cloud backups managed by the Network Manager/IT technician.)
- When I use my personal hand held / non Forest Way School devices in school (PDAs / laptops / mobile phones / USB devices/ tablets etc), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that I am given permission to connect to school ICT systems, they are protected by up to date anti-virus software and are free from viruses. I will not connect any personal devices to the school network without relevant permission.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not name my place of work on social networking sites such as Facebook.
- The school provides adequate data storage and remote access therefore e-mails should not contain images of pupils or personal or confidential information of staff or pupils.
- I will ensure that my data is available for regular backups (synchronising documents with server). The responsibility for data backup and disaster recovery will rest with the IT support manager.
- I will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others on school equipment or on personal equipment on school premises (eg child sexual abuse images, criminally racist material, adult pornography etc). I will not try to use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.
- Unless I have permission, I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on school systems, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- Access to management information systems will be tightly monitored and data will not be shared under any circumstances due to the sensitivity of the data.
- I will use the printers and photocopiers appropriately only printing when necessary and for school use only.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I will not bring the school into disrepute through the use of social networking sites such as Twitter, Google Plus and Facebook. I will not post photos, videos, comments or information related to the school or members of staff.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

21

Name _____

Signed _____ Date _____

22

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?	