TUTSHILL C OF E PRIMARY SCHOOL

WOOLASTON PRIMARY SCHOOL

Acceptable Use Policy

Approved by:	
Policy Lead:	
Date:	9th September 2024
Review Date:	

Contents

1.0 **Purpose of this policy**

- To educate pupils about e- safety issues and appropriate behaviours so that they remain safe and legal online.

- To help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.

- To keep any personal data and information secure.

- To minimise the risks of handling sensitive information.

2.0 **Scope of the Policy**

This policy applies to all members of our school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems.

The Education and Inspections Act 2006 empowers Executive Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. This policy has also been cross referenced to Keeping Children Safe in Education 2024.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

3.0. Introduction and aims

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's acceptable use provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Resources that could support e-safety teaching include:
- Be Internet Legends developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- Disrespectnobody is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
  - PSHE association provides guidance to schools on developing their PSHE curriculum
- Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
  - National Crime Agency/CEOPs education programme with age specific resources
  - UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors

- Establish clear expectations for the way all members of the school community engage with each other online

- Support the school's policies on data protection, online safety and safeguarding

- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems

- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

4.0 **Roles and Responsibilities**

The following section outlines the acceptable use roles and responsibilities of individuals and groups within the schools.

4.1 **Governors**:

Governors are responsible for the approval of the Acceptable Use Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Board has taken on the role of Safeguarding governor (which includes E-Safety). This role will include:

•   supporting the school to developing a whole school approach to online safety

•   regular monitoring of e-safety incident logs

•   ensure the schools have appropriate filters and monitoring systems in place

•   reporting to relevant Governors

4.2 **Executive Headteacher and Senior Leaders**:

• The Executive Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.

• The Executive Headteacher and Senior Leadership Teams should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).

• The Executive Headteacher is responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

4.3 **Executive Headteacher/ICT Coordinators**:

- Takes day to day responsibility for acceptable use issues and have a leading role in establishing and reviewing the schools' policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an acceptable use incident taking place.
- provides training and advice for staff
- liaises with the Local Authority and Focus Networks
- receives reports of e-safety incidents and creates a log of incidents to inform future acceptable use developments,
- meets regularly with the Safeguarding governor to discuss current issues, review incident logs and filtering control logs
- attends relevant meetings
- reports regularly to Senior Leadership Teams.

4.4 **ICT provider:**

The Executive Head teacher in conjunction with the IT provider is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority Acceptable Use Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with e-safety technical information in order to effectively carry out their acceptable use role and to inform and update others as relevant

- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Executive Headteacher for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies.

4.5 Teaching and Support Staff

Staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school acceptable use policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Executive Headteacher for investigation
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
-

4.6 Designated Safeguarding Leaders:

DSLs should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- child on child abuse eg through consensual and non-consensual photographs, cyber-bullying

4.7 Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's Acceptable Use Policy covers their actions out of school, if related to their membership of the school
-

4.8   **Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The schools will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

The school will therefore seek to provide information and awareness to parents and carers through:
- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

4.9   Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

5.0 Education & Training
5.1 Staff / Volunteers
 It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- A planned programme of formal e-safety training will be made available to staff. This   will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive acceptable use training as part of their induction programme, ensuring that they fully understand the school's acceptable use policy and acceptable use agreements.
- The Head teacher will receive updates through attendance at external training events   (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This acceptable use policy and its updates will be presented to and discussed by staff in staff meetings.
- The Head teacher will provide advice / guidance / training to individuals as required.

5.2   Training – Governors
Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:
- attend appropriate safeguarding and child protection training, including online safety at induction. This should amongst other things, include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- ensure online safety is integrated into the whole school approach to safeguarding.
- Attend training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participate in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

6.0 Filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their acceptable use responsibilities:

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority / other relevant body policy and guidance).

• There will be regular reviews and audits of the safety and security of school technical systems.

• Servers, wireless systems and cabling must be securely located and physical access restricted.

• All users will have clearly defined access rights to school technical systems and devices.

• The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Executive Headteacher or other nominated senior leader and kept in a secure place (eg school safe).

• The Executive Headteacher in conjunction with the LA Hardware support team is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

• Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details).

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

• A login is available for the provision of temporary access of "guests" (eg trainee teachers, supply teachers) onto the school systems.

• An agreed policy is in place (to be described) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

7.0 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

• In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

• Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website or Twitter or displayed in school.

8.0 Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Act 2018 which states that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Any breaches of GDPR regulations will be reported to the relevant agencies as soon as the school is aware.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It complies with General Data Protection Policy (see appendix for template policy)

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

9. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright

- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

- Breaching the school's policies or procedures

- Any illegal conduct, or statements which are deemed to be advocating illegal activity

- Online gambling, inappropriate advertising, phishing and/or financial scams

- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful

- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams

- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, its pupils, or other members of the school community

- Connecting any device to the school's ICT network without approval from authorised personnel

- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data

- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

- Causing intentional damage to the school's ICT facilities

- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation

- Using inappropriate or offensive language

- Promoting a private business, unless that business is directly related to the school

- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms

- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Executive Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

10.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

10.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies for example the behaviour policy and the staff code of conduct.

5. Staff Acceptable Use(including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school administrator manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices

- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the executive headteacher.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be sent via a secure email system such as Egress so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the executive headteacher immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The executive headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching time

- Does not constitute 'unacceptable use', as defined in section 4

- Takes place when no pupils are present

- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are not permitted to use their personal devices (such as mobile phones or tablets) during teaching times and during this time mobile phones should be on silent and kept out of sight.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1 and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited

- Bandwidth usage

- Email accounts

- Telephone calls

- User activity/access logs

- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The effectiveness of any filtering and monitoring will be regularly reviewed.

Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and ICT manager, as appropriate.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

The governing board will regularly review the effectiveness of the school's monitoring and filtering systems.

6. Pupils Acceptable Use

6.1 Access to ICT facilities

Laptops and ipads are only available to pupils under supervision of a member of school staff.

6.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents Acceptable Use

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity such as a parent governor may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through email and Tapestry messages.

7.3 Communicating with parents about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents in the same way that information about homework tasks is shared.

Parents may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All staff will be prompted to regularly update their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed the executive headteacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the executive headteacher immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

9. Protection from cyber attacks

The school will:

- Work with governors and the IT provider to make sure cyber security is given the time and resources it needs to make the school secure

- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email

    - Respond to a request for bank details, personal information or login details

    - Verify requests for payments or changes to information

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents

- Investigate whether IT software needs updating or replacing to be more secure

- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

- Put controls in place that are:
    - **Proportionate**: the school will verify this using a third-party through GCC, to ensure that what it has in place is effective
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Regularly back up critical data and store these backups
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to GCC.
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Work with Gloucestershire local authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school's wireless internet connection is secure. The school wifi can only be accessed via a password which is held by the school office. Pupils and visitors to the school will not be given the wifi password, IT equipment already linked to the wifi will be provided.

10.1 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The executive headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11 Reporting Breaches

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. **In the event of suspicion, all steps in this procedure should be followed:**
- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

12 Definitions

- **ICT facilities:** all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the school's ICT service

- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

13. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2024
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

13. Monitoring and review

The headteacher and governing board will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years by the governing board.

14. Related policies

This policy should be read alongside the school's policies on:

- e-safety
- Safeguarding and child protection
- Behaviour
- Staff code of conduct
- Data protection

Rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

2. Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional

3. Check your privacy settings regularly

4. Be careful about tagging other staff members in images or posts

5. Don't add parents and carers as friends

6. Don't share anything publicly that you wouldn't be just as happy showing your pupils

7. Don't use social media sites during school hours

8. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there

9. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)

10. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

11. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

- **Google your name** to see what information about you is visible to the public

- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

> In the first instance, ignore and delete the request. Block the pupil from viewing your profile

> Check your privacy settings again, and consider changing your display name or profile picture

> If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

> Notify the senior leadership team or the executive headteacher about what's happening

A parent adds you on social media

> It is at your discretion whether to respond. Bear in mind that:

- Responding to 1 parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

> If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

> **Do not** retaliate or respond in any way

> Save evidence of any abuse by taking screenshots and recording the time and date it occurred

> Report the material to Facebook or the relevant social network and ask them to remove it

> If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

> If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

> If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Acceptable use of the internet: agreement for parents and carers
Name of parent/carer: **Name of child:**

Online channels are an important way for staff to communicate with parents/carers about our school.

The school uses the following channels:

- Tapestry (EYFS)
- SeeSaw (Yrs 1 – 6)

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way
- Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers

Signed:	**Date:**

**Acceptable use of the school's ICT facilities and internet:
agreement for pupils and parents/carers**

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 4 : Acceptable and Unacceptable User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
On-line gaming (educational)			X	X		

On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps		X	X		
Use of video broadcasting eg YouTube		X	X		

Appendix 5 : guidelines for use of personal communications

Use of Communication Technologies	Staff and other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X	X			X	X	x	
Use of mobile phones in lessons		X	X					x
Use of mobile phones in social time	x				x			x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices eg tablets, gaming devices				x				x
Use of personal email addresses in school, or on school network				x				
Use of school email for personal emails				x				x
Use of messaging apps		X						X
Use of social media		X						X
Use of blogs		x						x

Appendix 6 : Flow Chart for Reporting Actions

```
                        ┌──────────────────────┐
                        │ Online Safety Incident│
                        └──────────┬───────────┘
              ┌────────────────────┴────────────────────┐
              ▼                                          ▼
     ┌─────────────────┐                    ┌──────────────────────┐
     │Unsuitable Materials│                  │ Illegal materials or  │
     └────────┬────────┘                     │ activities found or   │
              ▼                              │ suspected             │
     ┌─────────────────┐                     └──────────┬───────────┘
     │Report to the     │          ┌──────────────┬─────┴──────┬──────────────┐
     │person responsible│          ▼              ▼            ▼
     │for Online Safety │  ┌──────────────┐┌──────────────┐┌──────────────┐
     └────────┬────────┘   │Illegal Activity││Illegal Activity││Staff/Volunteer│
              ▼            │or Content (No  ││or Content (Child││or other adult │
     ┌─────────────────┐  │immediate risk) ││at Immediate Risk)│└──────┬───────┘
     │If staff/volunteer││└──────┬───────┘└──────┬───────┘        │
     │or child/young    │       ▼                │          ┌──────────────┐
     │person, review the│ ┌──────────────┐       │          │Report to Child│
     │incident and decide││Report to CEOP │       └────────►│Protection team│
     │upon the          │ └──────┬───────┘                  └──────┬───────┘
     │appropriate course│        │                                 ▼
     │of action, applying│       │                          ┌──────────────┐
     │sanctions where    │       │                          │Call professional│
     │necessary          │       │                          │strategy meeting │
     └──┬──────────┬────┘        │                          └──────┬───────┘
        ▼          ▲             │                                 │
  ┌──────────┐ ┌──────────┐      └─────────────┬──────────────────┘
  │Debrief on │ │Record     │                   ▼
  │online     │ │details in │            ┌──────────────┐
  │safety     │ │incident   │            │Secure and     │
  │incident   │ │log        │            │preserve evidence│
  └────┬─────┘ └────┬─────┘             └──────┬───────┘
       ▼            ▼                           ▼
  ┌──────────┐ ┌──────────┐            ┌──────────────┐
  │Review     │ │Provide    │           │Await CEOP or  │
  │policies   │ │collated   │           │Police response│
  │and share  │ │incident   │           └───┬──────┬───┘
  │experience │ │report logs│               ▼      ▼
  │and        │ │to LSCB    │
  │practice as│ │and/or     │
  │required   │ │other      │
  └────┬─────┘ │relevant   │
       ▼       │authority  │
  ┌──────────┐ │as         │
  │Implement  │ │appropriate│
  │changes    │ └──────────┘
  └────┬─────┘
       ▼
  ┌──────────┐
  │Monitor    │
  │situation  │
  └──────────┘
```

Boxes (transcribed):

- **Online Safety Incident**
- **Unsuitable Materials**
- **Illegal materials or activities found or suspected**
- **Report to the person responsible for Online Safety**
- **Illegal Activity or Content (No immediate risk)**
- **Illegal Activity or Content (Child at Immediate Risk)**
- **Staff/Volunteer or other adult**
- **If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary**
- **Report to CEOP**
- **Report to Child Protection team**
- **Call professional strategy meeting**
- **Debrief on online safety incident**
- **Record details in incident log**
- **Secure and preserve evidence**
- **Review policies and share experience and practice as required**
- **Provide collated incident report logs to LSCB and/or other relevant authority as appropriate**
- **Await CEOP or Police response**
- **Implement changes**
- **If no illegal activity or material is confirmed then revert to internal procedures**
- **If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body**
- **Monitor situation**
- **In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action**

Appendix 7: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.