Emersons Green Primary School

ICT Security Policy

Ratified:	June 2023
Review:	June 2024

Equality Statement

At Emersons Green Primary School we are committed to ensuring equality and opportunity to all members of our school community. In regard to ICT Security, the school always aims to ensure that no one is treated less favourably than anyone else. The Equality Act 2010 defines these responsibilities. In regard to this, this Policy, including all of its procedures and systems will have due regard to:

- Eliminating discrimination and other conduct prohibited by the Equality Act
- Advance equality of opportunity between people who share a protected characteristic and people who do not share it
- Be aware of this duty to have due regard when making decisions or taking action in order to assess whether that action will have implications for people with protected characteristics
- Consider equality implications before and at the time that this policy is developed and reviewed and keep these implications under review on a regular basis

It is unlawful to discriminate in the following areas, termed protective characteristics (all Safeguarding policies, procedures, systems and actions must take this into account):

- Age
- Disability
- Gender
- Gender reassignment
- Marriage and civil partnership
- Pregnancy and maternity
- Race
- Religion or Belief
- Sexual orientation

Aims of this Policy

This policy applies to all schools, all staff, students, and governors as well as guest users at Emersons Green Primary School.

The objectives of the Policy are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.
- To specify minimum standards that constitute acceptable use of ICT systems.

'Information' covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

In school, the Head of Schoo has overall responsibility for managing the security of the IT network, delegated to the School Business Manager. The school's ICT Provider (Integra) has delegated responsibility for the school's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The ICT Provider (Integra) is responsible for systems that constantly monitor the security of the network and systems that form the school's IT network.

The ICT Provider (Integra) will inform the school of any data security issues involving the school. The ICT Provider (Integra) must be informed by the school of any information security issues.

Responsibilities:

- Users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy
- Users are responsible for notifying the Head of School and School Business Manager of any suspected or actual breach of ICT security; a log of security or privacy breaches will be made in the relevant register, to comply with GDPR.
- Users must comply with the requirements of the Data Protection Act 2018, Computer
- Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Adequate procedures must be established in respect of the ICT security implications of personnel changes.

Procedural Aspects of the Policy

The **Governing Body** must ensure that the school implements an ICT Security Policy. This must be reviewed annually.

The **Head of School** delegates day-to-day responsibility for data security to the **School Business Manager**, who coordinates directly with the ICT Provider (Integra). The Head of School must ensure that the nominated member(s) of non-teaching staff understands the functions of the role and is familiar with the relevant Acts.

The **School Business Manager** should ensure that a copy of the relevant Acceptable Use Policy is made available to all users and that users are periodically reminded of their obligations under this policy. This should include all relevant aspects of the ICT Security Policy

and any other information on the use of facilities and techniques to protect the systems or data.

The **School Business Manager** should retain a record of

- the access rights to systems and data granted to individual users;
- any amendments or withdrawal of these rights due to a change in responsibilities or
- termination of employment or starters/leavers;
- the training provided to groups and individual users in regard to data security.

An inventory of all ICT equipment must be maintained and regularly updated by the **School Business Manager** as equipment is purchased/disposed of. The inventory must be checked and verified annually in accordance with the requirements of financial regulations. The **School Business Manager** must ensure there are clear procedures regarding the disposal of equipment containing confidential or sensitive data; such procedures must be compliant with the Waste from Electronic and Electrical Equipment (WEEE) directive and that that third parties involved in the disposal of equipment are registered under the Data Protection Act as personnel authorised to see data; as such they will be bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

An inventory of all software and licence details must be maintained and regularly updated by the **School Business Manager** as software is purchased/disposed of. The inventory must be checked annually to ensure that the licences accord with installations.

The **ICT Provider (Integra)** should ensure there are clear procedures regarding the installing/copying of software.

The **School Business Manager** should undertake a 'password strength checking exercise' twice per year, to identify any weak passwords being used by staff to protect sensitive data and rectify security weaknesses as soon as possible.

The **ICT Provider (Integra)** must ensure that "shared passwords" – such as those used by ICT support staff to administer school servers, are

- sufficiently complex to satisfy industry best practice on security
- stored in password management software that utilises strong encryption

The **ICT Provider (Integra)** has a policy on anti-virus software for local networks, stand-alone systems, laptops and privately-owned devices used to access school networks. This must ensure that antivirus software is regularly updated, suitable for the task of identifying malware and protecting school systems and data from malware attacks.

Firewall, Anti-virus and Backup Strategy

Integra Firewall system:
At the core of the Broadband Infrastructure subscribed to is a fully secured SD-WAN which is firewalled and secured at the perimeter via nextgen Palo Alto firewalls.

Integra Backup systems:
There is no data stored on the school site. All the server infrastructure that supports schools is accommodated in council facilities. The live production data is housed in South Glos Badminton Road offices, which have full uninterruptable power supplies together with generator back-up. In the main server room there are fire suppression systems which will extinguish fire without damage to the infrastructure. This is where all school data is secured. It is also where the council's corporate IT function house their main facilities. The off-site

backup facility is in Kingswood Civic Centre, where which houses data backups as well as facilities in light of a potential failure at Badminton Road. Access to both are restricted to only a few members of both the Corporate and Schools IT (Integra).

In the near future Integra will be migrating all live systems to an N+1 data centre which sits within the core of the school's network in Maidenhead (with full ISO27001 accreditation), and moving the backup facility to Badminton Road, all for improved resilience and security.

At the core of Integra data protection, there are storage-level snapshots, which has been increased by 50% to continue accommodating this. These snapshots are a crucial first-line to swift recovery.

Integra use a Dell IDPA5500 EMC PowerProtect appliance, using Avamar software, for backups. This is a hardened product set with proprietary protocols and is a tried and tested level of protection. Integra are currently using Microsoft Data Protection Manager to perform backups (there is a plan for this to be phased out in favour of the Dell Solution). Full offline backups are then offloaded to cloud storage for complete separation from the network.

End user devices are fully managed, all security patches are applied and antivirus software updates applied in real-time when new viruses are encountered. All devices are encrypted to ensure security of resting data, and any remote access is fully encrypted and secured.

Microsoft 365 cloud provision is not backed up, but there is a retention period of 90 days for any data deleted. Microsoft offer resilience through its network in terms of data centre failover, but do not offer a backup on the service by default.

Personal Devices Policy

The school may allow personal devices to be used on an individual basis, although this must be agreed with the Head of School and School Business Manager. Any personal device will only be able to be connected to the internet and will not have access to the school network.

At Emersons Green Primary School, some pupils have AAC (Augmentative and Alternative Communication) devices provided by an approved external professional organisation (e.g. AAC West), that are considered personal devices, as they are not provided by the ICT Provider (Integra). These devices will be approved by Integra, who will link them to the internet for pupil usage. These devices will not be linked to the school network. The preferred method of us for these devices is to utilise cloud storage for file transfer. Should a physical memory device need to be used, then it must be provided by the school and not used in any other device.

Acceptable Use

The school defines acceptable use as activities that directly or indirectly support the students' education.

The school defines acceptable personal use during work time as reasonable and limited personal communication or recreation, using personal devices.

Employees and students are blocked from accessing certain websites during work hours/while connected to the school network. This is a default set up by the ICT Provider (Integra). Employees may occasionally be permitted to have access to default-blocked website for educational purposes, at the discretion of the Head of School. The Head of School and

employee will check the website content and the Head of School will email the ICT Provider (Integra) to confirm.

Work devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others
- Engage in external business activities
- access personal accounts such as Social Media, shopping, booking events etc.

Staff may use their mobile device to access the following school-owned resources: Outlook email, Outlook calendars, documents (e.g. through email) and software packages such as Arbor and CPOMS (where licensing restrictions permit) subject to restrictions on time and location of mobile phone use.

Full Acceptable Use Policies for Staff, pupils and parents are attached as Appendices to this Policy.

Mobile Devices

Pupils may not use mobile phones within the school site. Any pupil bringing a phone to school must put it in a box in the teacher's cupboard during the school day. Pupil mobile phones will not be linked to the internet or school network.

Staff and visitors are not permitted to use their mobile phone during the school day, unless in a private space and authorised by a member of SLT. Mobile phone use is permitted in the staff room. Staff and visitors are otherwise expected to leave the building to use their phones. Staff and visitor mobile phones will not be connected to the internet or the school network.

Staff who use school iphone and other portable devices will use them for work purposes only, whether on or off of the school premises. Staff will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, politically/ religiously extreme material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. The iphone will remain in the 'custody' of school staff throughout a trip/visit and will be returned to the school office upon return or as soon after any images have been downloaded to the school network.

Device Security and Passwords

In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the school's network.

Work computers can only be accessed by pressing CTRL+ALT+DEL to login.

When an individual signs out, or the computer is restarted, the previous logged-on user name will not be displayed. The new user will need to enter their username and password each time to login.

Passwords must be changed regularly. See below for Password policy.

Computers will automatically lock themselves if they are idle for 15 minutes. The user must re-enter their password to resume working.

Staff and pupil access to school data will be limited, based on user profiles defined by our ICT Provider (Integra) and automatically enforced.

Risks/Liabilities/Disclaimers

The school reserves the right to disconnect devices or disable services without notification.

Lost or stolen devices owned by the school must be reported to the Head of School/School Business Manager and the ICT Provider helpdesk (Integra) as soon as possible. Privately-owned devices that contain data owned by the school that have subsequently been lost, must also be reported to The Head of School (e.g. documents as part of work emails).

If a device containing personal data has been lost or compromised, then the school must report to the Data Protection Officer and the Information Commissioner's Office. Please see the whole school Data Protection Policy for more information.

The member of staff or pupil is expected to use his or her devices in an ethical manner at all times and adhere to the relevant Acceptable Use Policy.

The member of staff has no personal liability for costs associated with his or her device.

Emersons Green Primary School reserves the right to take appropriate disciplinary action should a member of staff's actions result in data loss, device damage or otherwise compromise of hardware or data.

Security & safety requirements for ICT systems

Password policy
Emersons Green Primary will enforce a policy of strong passwords for all staff users and users with elevated privileges, on the grounds that they regularly have access to sensitive personal information. Staff passwords should:
• Be alphanumeric, including a mix of upper and lower case letters – **ideally using 'three random words' e.g. TreeCatPlan**
• contain at least one "special character" (such as $, %, #, ?, ! etc)
• at least 8 characters in length
Passwords should never be:
• written down
• easy to guess (e.g. Johnsmith1 or Johnsmith1@)

Staff users will be required to change their password(s) in situations where the ICT Provider (Integra) identifies that weak passwords have been used, or where it is known or suspected that a user's password may have been compromised by unauthorised third parties.

Changed regularly.

Supply teacher passwords
Supply teachers and other regular non-staff users of the network (such as Sports Coaches, teacher training students) can be issued with a 'supply' login and password.

These passwords are generated automatically at 4.30pm on the previous day (including Saturday for Monday morning) by the ICT Provider (Integra) and are automatically saved into the Teachers (J Drive) which can only be access by school staff. These passwords expire on

4.30pm on each day. These passwords give users access to the main school network, but no printing privileges or access to secure Drives or folders

Unattended workstations
Staff screensavers will lock with a password after 15 minutes of inactivity. Staff must be mindful of what is being displayed on their screen and who can see it; leaving unlocked workstations with sensitive data such as email or personal data must be avoided. Laptops should be closed when unattended.

Portable media and Remote Access
School staff have access to a secure, online remote access to the school network. This is the strictly preferred method for staff to access school information outside of the workplace. Remote access can only be made through work devices, as they are the only devices which contain the required VPN (Virtual Personal Network). If a member of staff accesses remote access using a personal device, then they must ensure the network connection is secure. If staff utilise remote access through a shared public network (e.g. café or airport) the connecting should be secure, as the remote access system uses a secure VPN link.

Portable media such as USB devices or external hard drives may need to be used within school to transfer information between work devices and personal devices (e.g. pupil AAC devices). In this case, the USB device must be provided by the school and it must not be used in any other device.

Portable media such as USB devices may be only be used to transport files between work and external locations if approved by the Head of School. Any such devices must be password protected/encrypted and provided by the school.

Personal USB devices or external hard drives must not be put into school devices (at work or outside of the workplace) without permission, as there is a risk of transmitting viruses etc. Any files containing personal information or other sensitive data may only be transported outside the school on encrypted devices. These devices should be virus-scanned each time they are inserted into a device connected to the school network – this option is given on devices when an external memory device

When disposing of legacy portable hardware that may not have been encrypted in the past, staff should seek advice from the School Business Manager, who will coordinate with the ICT Provider (Integra) to ensure that any sensitive data is securely erased before disposal.

File-type & software restrictions
The ICT Provider (Integra) will ensure appropriate security policies are in place to prevent unauthorised users from using file types that could bypass security measures or otherwise cause security problems. Should this be detected then the school will be informed.

Physical security
As far as practicable, only authorised persons will be admitted to rooms that contain servers The on-site server and network is monitored remotely by the ICT Provider (Integra) in order to identify potential unauthorised access to the network or network/internet failure. In such cases, the ICT Provider will contact the school and action will be taken to secure the school network.

Internet use & Filtering

The ICT Provider (Integra) will ensure that appropriate firewalls are in use at the extremities of the school networks to guard against nefarious actors gaining unauthorised access to school systems.

Filtering proxy servers will also be used to ensure that all internet traffic is age-appropriate, safe to use and logged.

Where staff or visitors become aware of inappropriate material being accessed on school systems, this should be reported to the school office. The school must inform the Headtacher and report to the ICT Provider (Integra)

A number of websites are automatically blocked by the ICT Provider (Integra) who can unblock access at the discretion of the Head of School. Any website that is unblocked muts be checked by the Head of School and another member of staff to ensure it is safe, before a request is made to the ICT Provider (Integra).

The school Acceptable Use Policy (AUP) is available as part of this document for staff, parents/carers and pupils (see Appendix). All persons using the network will be required to accept the AUP before they logon.

Parental permission will be required before any student is allowed to use school ICT facilities; this is managed through the home-school agreements and pre-admission procedures for the school. All parents are provided with the Acceptable Use Policy when their child starts the school.

Monitoring system usage

Emersons Green Primary School is mindful of its obligations in regard to the monitoring of data on the school network and the potential for monitoring activity to contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act, 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring.

The ICT Provider (Integra) support staff will be mindful of their obligations under law, including the Data Protection Act (2018) which incorporated the General Data Protection Regulations (GDPR) into UK law.

The monitoring of ICT system use for school business will be reasonable and proportionate, for the purposes of protecting pupils, staff or visitors from harm; complying with the law; and preventing unauthorised access to school ICT systems or private information.

In order to facilitate the monitoring of internet traffic the ICT Provider (Integra) monitor the system remotely and may also come on site to carry out further monitoring activities.

The Head of School and School Business Manager should coordinate with the ICT Provider (Integra) ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Users should be aware that the protocols discussed here in Monitoring system usage apply to all internet traffic at all times on school devices workstations.

Pupil use of devices and the internet will be monitored directly by adults.

Rules for ICT use by third parties

Under some circumstances, it may be desirable to grant third parties (that is, people who are not staff, governors or pupils) access to school ICT systems, such as ICT service providers (with the permission of the existing ICT Provider), other service providers (e.g. printer supply company), supply teachers, potential staff attending interview or pre-employment induction, or potential pupils.

.

In general,

- Access must only be made via the provided authorised account and password, which must not be given to any other person.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area, as assigned by the school. Such files will be regularly removed from the system.
- The school ICT systems may not be used for private business purposes, unless the Head of School has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in access privileges being revoked and could be used to inform decisions about potential employment or acceptance in the case of candidates for employment or admission.
- Non-school devices must not be connected to the school network without permission and being checked for safety by the ICT Provider (Integra). External memory devices which have not been provided by the school must not be connected to school devices. The ICT Provider (Integra) has advised that the safest way to transfer this information is via email, although staff must only open attachments or download files if they are sure it has come from a secure source.

Guidance for best practice for staff communication is included in the appendix: ‘E-mail & Internet use: good practice for staff’ and for Classroom monitoring of students’ ICT usage as is the Acceptable Use Policy.

Appendix A:

Classroom monitoring of pupil ICT usage

- Staff should ensure they are able to visually monitor pupils' use of computers at school and that there is always a responsible person present.
- Monitoring software may be used to facilitate in-lesson monitoring by teaching staff.
- The ICT Provider (Integra) will log and monitor access to the network remotely, and in particular, logs of network and internet traffic will be kept for the purposes of generating an audit trail of pupil and staff ICT usage.
- Where staff or pupil use of ICT systems could constitute illegal activity, staff are duty bound to bring this to the attention of the Head of School or other members of the Senior Leadership Team so that appropriate action can be taken.
- Where staff identify activity that constitutes a Safeguarding concern, they must immediately raise this with the Designated Safeguarding Lead (Head of School) or other member of SLT.
- Should inappropriate content be detected on a device, the device must not be switched off. It must be immediately removed from the vicinity of children and then given to the Head of School/School Business Manager, so the content source can be identified. Laptop lids can be closed or other devices switched into sleep mode.

Appendix B: E-mail & Internet use: good practice for staff

The following guidelines (some of which also apply to other forms of correspondence) advise what

- is and what is not good practice when using e-mail and other similar systems to communicate.
- Staff should:
- treat E-mail as they would a letter, remembering that they can be forwarded/ copied to
- others;
- only contact children's family members for professional reasons and in accordance with school policy. DO not directly contact pupils.
- use "BCC" fields when addressing emails to multiple recipients whose confidentiality needs
- to be maintained.
- only click on a link or open a file if they are sure it comes from a trusted source. If a member of staff is concerned about the content of an email, particularly if it contains unsuitable content, a possible virus or may be a phishing email, then this must be reported immediately to the Head of School/School Business Manager who can then coordinate with the ICT Provider (Integra) the check the security of the email.

Staff should not:

- use internet or web-based communication channels to send pupils messages of a
- 'personal' nature
- use or access social networking sites of children or young people. Staff may be 'friends' with parents or carers if they have an existing relationships with those individuals outside of the workplace.
- use internet or web-based social media channels to bring South Gloucestershire Council or the school's name into disrepute.

Staff conduct on any social media, forums etc. must be in line with the Staff Code of Conduct.

Please also see the **Acceptable Use Policy (Staff)** and the **Staff Code of Conduct.**

Appendix C: Acceptable Use Policy (Staff)

Acceptable Use Policy Agreement

Content

- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I know that internet use is proactively monitored and any illegal activity will automatically result in police involvement
- I will not make large downloads or uploads that might take up internet capacity.

Contact

- I will communicate online in a professional manner and tone and I will not use aggressive or inappropriate language and am aware that any communication could be forwarded to an employer or governors.
- I will only communicate with students / pupils and parents / carers using official school systems.
- 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 only use my own user names and passwords which I will choose carefully so they cannot be guessed easily.
- When carrying out video calls I will use an appropriate background, appropriate dress and carry this out in an appropriate location.

Social Media

- I will only use chat and social networking sites for school purposes that are approved by the school.
- When using social networking sites and other services for personal use I will not say anything that could bring the school, staff members or any member of the school community into disrepute.
- I will ensure that I do not refer to students, pupils, parents/carers or school staff.
- I will not engage in any online discussion about the school or any members of the school community unless this is in an approved context e.g. school own Facebook page
- I will not attribute my personal opinions to the school on sites and will make clear that they are my own opinions
- I will immediately report any online discussion that could impact on the school / staff reputation and any negative postings about any member of the school community
- I will not ‘friend’ students on social networking sites.
- I will not friend parents/carers on social networking sites, unless there are exceptional circumstances agreed by the Head of School (e.g. member of staff is also a parent/carer at the school, member of staff was parent/carer at the school prior to becoming a member of staff, member of staff is a part of the local

community). Staff members must not routinely 'friend' parents or carers. If I believe there are mitigating circumstances that may allow this, I must:
    - Inform the Head of School
    - Apply this policy to all my behaviours using this aspect of social media (e.g. do not bring the school into disrepute, do not breach confidentiality). My behaviour on social media must match my professional behaviour outside of social media.
    - Monitor this aspect of my own online behaviour and immediately report to the Head of School if I believe there is an incident that actually, or appears to, compromise my professional responsibilities.
    - Accept that if there is evidence that this aspect of online behaviour breaches this policy and/or the school code of conduct, then there will be a disciplinary investigation carried out by the school.
- I must also be aware that I may inadvertently reveal personal information about other members of staff through social media, e.g. by 'liking' their posts, which makes those posts visible to other people. This must not occur as it breaches the privacy of other staff. I will not 'like' private posts of staff if this will then occur.
- Members of staff may create social media posts promoting the work of the school via the school's official Twitter account. However, the following restrictions apply:
    - Staff should only take photos of children using school equipment e.g. a school phone or tablet.
    - Staff should only take photos of children whose parents have given permission for their images to appear on Twitter (permissions for this will be sought annually via Arbor).
    - Staff will not put children's names next to photographs.
    - The school's Twitter account will be locked and only visible to parents who have been given permission to view it.

Conduct

- I will only use school equipment for the purposes of school business.
- I will not engage in any on-line activity that may compromise my professional responsibilities or compromise the reputation of the school or its members. This includes use of the school e-mail account, logo or my school role.
- Filtering is provided through the South Gloucestershire internet service. I know that, as a staff user, I have access to resources that learners cannot access for teaching purposes.
- I will not try and bypass this filtering or access sites that are illegal.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement when using it.
- I will not use my personal equipment to record and store images / video of children.
- I will only take images or video of pupils/staff where it relates to agreed learning activities and will ensure I have parent/staff permission before I take them. If these are to be published online or in the media I will ensure that parental / staff permission allows this.
- Where images are published (e.g. on the school website) I will ensure it is not possible to identify the people who are featured by name or other personal information.

- I understand my photograph may be used on the school web site, which means that it could be copied by others. I know that where it is used my photograph will not be accompanied by any personal details.
- I will not install or store programmes on a school device unless I have permission.
- I will not try to alter computer settings, unless this is allowed in school policies.
- I will not cause damage to ICT equipment in school and will immediately report any damage or faults involving equipment or software.
- I will not access, copy, remove or otherwise alter any other user's files, without their permission.

Mobile Phones

- I will ensure that I have permission to use the original work of others in my own work and will credit them if I use it. Where work is protected by copyright, I will not download or distribute copies (including music and videos). I will not use my mobile phone in the presence of children. Any use of mobile phones must occur outside of pupil contact time or in a private location (e.g. staff must leave the building).
- I will not take any photos of children using my mobile phone.
- If I have a mobile phone on site, I will keep it stored away and not bring it out unless I have left the building or it has been agreed by a member of the senior leadership team that I may use it in a private location (e.g. in the case of an emergency).
- I am aware that there may be sanctioned times to use a mobile phone, for example when on a residential trip if there is an emergency.

Data Protection

- I understand that our school only uses services which mean that data is stored in line with GDPR guidelines.
- I have read the GDPR guidance leaflet and signed to say I understand my responsibilities.
- When I use a device e.g. laptop at home I will ensure resources cannot be accessed or copied by anyone else and that no one else uses the laptop.
- I will ensure personal equipment used is password protected.
- I will ensure that my data is regularly backed up.
- I will take all steps within my power to keep personal data safe and minimise the risk of losing it.
- I will only use personal data on secure devices that are password protected.
- When transferring data I will use encryption and secure password protected devices.
- I will ensure that devices I use have approved virus and malware checking software and I will delete data securely once it has been transferred or finished with
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when I am required by law or by school policy to disclose it to an appropriate authority.
- I will not send personal information by e-mail if it is not secure. I will use secure communication systems, such as SOFIE or remote network access, as advised.

Use of Staff Images on School Publicity and Web sites

- I understand my photograph may be used on the school web site, which means that it could be copied by others. I know that where it is used my photograph will not be accompanied by any personal details other than my title and surname.

Promoting Safe Use by Learners

- I will model safe use of technologies and the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school policy if an issue arises in or out of school that might compromise learner, user or school safety; or if a child reports any concerns.
- I will monitor learner behaviour online when using technology and deal with any issues that arise.

Problems

- I will immediately report any illegal, inappropriate or harmful material; or incident I become aware of, to the e-safety co-ordinator or Head of School.
- If I believe a member of staff is infringing this policy, or putting themselves or others at risk, I will report this to the Head of School.
- If I believe a young person may be at risk I will follow the safeguarding and child protection procedures (see Child Protection and Safeguarding policies)
- If I believe a young person may be being bullied via technologies I will follow the Anti-bullying Policy.

Appendix D - Acceptable Use Policy (Parents):

Parent / Carer Acceptable Use of IT Policy

Technologies open up new learning opportunities and can promote creativity, effective learning collaboration and communication. They can promote more effective communications between parents / carers and the school in order to support young people with their learning. This Acceptable Use Policy is intended to ensure:

- You are aware of what the school is doing to help your child become a responsible user of technology and stay safe at school
- You are aware of the importance of e-safety and are able to support your child with keeping safe and behaving well online at home.

The school will aim to ensure your child has good, safe access to IT for learning and, in return, expects your child to use the equipment responsibly.

Content

- We only allow children to use age appropriate web sites in schools as using sites for older users can increase the risks to them. We accept that you may allow them to use sites that they are not old enough for at home. If this is the case then we would hope that you will be monitoring their use and will deal with any issues that arise.
- The school takes every reasonable precaution, including monitoring and filtering systems, to ensure that your child is safe when they use technology at school. The school cannot be held responsible for the nature and content of all materials that are accessible using technology as security systems cannot protect against everything.

Contact

- Children and members of staff may use digital devices to record learning activities. These images may be used in lessons or to celebrate success through being published in newsletters, on the school website, Twitter or occasionally in the public media.
- The school Twitter account will be used to celebrate learning and share events. The account is locked and is only viewable by permitted 'followers'. The school will only allow parents, vetted agencies and other schools to view the school's Twitter account.
- The school will comply with the Data Protection Act and ask your permission, through this policy, before taking images. We will also ensure that when images are published the young people cannot be identified by the use of their names, e.g. by publishing names alongside. Permission for children's images to appear on Twitter will be explicitly sought.
- If you take images at school events which include children, other than your own, you will need to follow these guidelines. Your child should also only take and use images with permission.
- School policy requires that staff do not make contact with parents or children through personal social networking sites or personal e-mail addresses but only through agreed school systems. This being the case we hope you will respect this by not requesting to be friends with staff on social networking sites and will understand if staff refuse any friend requests that are made.

Conduct

- Your child is expected to behave well online as they are expected to during all other school activities.
- Bullying is not tolerated in any form and this includes online 'Cyber-bullying'.
- Your child will be asked to sign the attached Acceptable Use Agreement which sets out clear expectations of behaviour when working online. We hope you will talk to your child about this.
- Your child will be taught about e-safety and keeping safe using technology.
- They should only use their own log in for systems and to keep their details private. Your child is responsible for anything their log in is used for.
- Your child's use of IT in school will be monitored and we will contact you if we have e-safety concerns.

Problems

- We can only take responsibility for e-safety issues that happen in school, or at home when children are using sites recommended by the school. However, the school retains the right to sanction children in school for serious breaches of e-safety/ cyber-bullying at home where these have had a detrimental effect on learning or has brought the school's reputation into disrepute.
- You are obviously responsible for your child's safety online when at home and we would hope you will be discussing e-safety with your child and monitoring their use of computers and mobile phones.
- Any issues you are made aware of with use of technology in school should be reported immediately to a child's teacher so that appropriate steps can be taken.
- If your child does not behave appropriately online then the school will take steps to deal with this as with any other issue with behaviour.

Permission Form

We request that you sign the parental consent on Arbor to show your support of the school in helping to keep your child safe. By consenting you are agreeing that:

- Your child can use school IT systems for systems
- You have read and discussed the rules with your child
- You understand the rules that your child should be following when using IT in school and this also applies to their use of their mobile phone
- You give permission for taking and using images of your child for learning purposes

Home Use of the Internet

We hope you will reinforce the e-safety messages when your child uses the internet at home. Some ways that you could do this are listed here to support those of you who may not be aware of all the issues. You will want to make sure that your child has appropriate supervision for their age. With the large number of mobile devices it is now very difficult to supervise all access to the internet, however you will want to ensure that you discuss what is appropriate. This means setting appropriate rules for using IT at home. The school rules could be a starting point.

Content

- Make sure content is appropriately filtered for younger users.

- Make sure your child knows that a protection system does not stop all unsafe content and they need to tell you if they access something inappropriate or get an upsetting message.

Contact

- Talk about the need to be polite online and that they should not use bad language or comments which might upset others.
- Discuss the fact that e-mails / messages/ social media posts can be intercepted and forwarded on to anyone (including parents, head teacher or future employer).
- Make sure they know they should not open messages if the subject field is offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.
- Monitor children's online gaming, including on games consoles as these often contain unfiltered communication with strangers.

Conduct

- Talk to your child about the fact that any information published on the web/ social media can be read by anyone and that they should only post things they would be happy for anyone to read.
- Check that they are old enough for the sites/apps/ games they are using. If you allow them to use a site/app/game they are not old enough for ensure that you have access to what they are doing so that you can monitor it.
- Make sure that family computers are password protected and have anti-virus software which is regularly updated.
- Make sure that digital devices used by the child (tablets, phones, games consoles) have parental controls set to filter and block inappropriate content.
- Ensure that your child knows not to leave computers logged on with their user name or logged on to sites with personal details entered as others could use them. Discuss user names and talk about how to choose them carefully to protect their identity.
- Talk about the information children should keep private in order to stop them being contacted including full name, address, telephone no, school, places they go regularly, etc. Check information that younger users are publishing to ensure that they are not putting themselves at risk. This includes any personal information which could lead to someone being able to contact them.
- Ask your child about the sites they are visiting, apps that they are using & games which they are playing.
- Talk about the need to use the safety and privacy features of sites/apps/ devices to only give access to people they know and being careful who they add as friends.
- Make sure they know that downloading copyrighted games/ media without paying for it is illegal.
- Discuss how to recognise commercial uses of the internet e.g. iTunes, mobile phone downloads, etc. Remind them they should not respond to offers they have not requested as these could be scams, result in costs or be trying to find out their personal information. Remind them that they should not purchase or download anything that costs money without asking permission and that they should not use someone else's identity to buy things online.

Problems

- Make sure they know that if they get any problems with using computers or get an offensive or worrying message / post/ e-mail they should not reply but should save it and tell you.
- Please tell the school of any concerns that you have or anything that they could help to address through teaching.

Rules for Keeping Safe with IT

EYFS & Key Stage 1

- I will ask a teacher when I want to use the computer or contact people using IT.
- I will only use a computer when an adult is present.
- I will only use the web sites, apps and games that I am allowed to.
- I will keep my password secret and not tell it to anyone.
- I will be polite and friendly when I use the computer to contact people.
- I will keep my personal details secret and not tell anybody about my home, family and pets. I will keep my friend's details secret too.
- I know that things I put up on the internet can be seen by anyone and I will not upload anything without asking an adult first
- I will not take or share pictures of anyone without asking them first.
- I will check information I find online as it might not be true.
- I know that I should not buy anything on line.
- I will tell a teacher (or adult I trust) if I find anything on a computer/ tablet/ phone or a message that is mean, upsetting or worrying.
- I will tell a teacher (or adult I trust) if I know of anyone that is behaving badly on line or if I know anyone may be being bullied.

I will use IT by these rules when:

- I use school IT or my own in school
- I use my own IT out of school to for school activities

If I deliberately break these rules then I know that there will be consequences.

My Name is

My Class teacher is

Signed

Date

Key Stage 2 - Rules for Keeping Safe with IT

Content

- I will use clear search words so that I find the right information.
- I know that some content may not be filtered out and what to do if I find something worrying.
- I will double check information I find online.

Contact

- I know that I need to behave well online as in real life and be polite and friendly.
- I know that if I am rude or bully someone online at home, I may get into trouble at school.
- I will not open messages if the subject field is not polite or if I do not know who it is from.
- I am careful about what I send as messages can be sent on to my parents or head teacher.
- I know that I must have permission to communicate online and will make sure my teacher / parents know who I communicate with.
- I will talk to an adult if an online friend wants to meet me and never arrange to meet anyone without permission.
- I know that anything I put up on the internet can be seen by anyone.
- If I bring my mobile phone to school I will give it to the teacher at the beginning of the day and not use it at all in school.

Conduct

- I will not use IT in school (including my own) without permission from my teacher.
- I will choose my user names and passwords carefully to protect my identity and I will not share them. I will not ask computers to remember my password.
- I know I must keep my personal details and those of others private.
- I will not visit unsafe sites or register for things I am not old enough for.
- I will log off sites when I have finished.
- I know that I should not buy anything on line without permission.
- I will not use anyone else's work or files without permission.
- Where work is protected by copyright, I will not try to download copies.
- I will not take or share pictures of anyone without their permission.

Problems

- I will not try to change computer settings or install programmes.
- I will not damage equipment and will tell a teacher if equipment is broken or not working.
- I will tell a teacher or adult I trust if I find anything on a computer or message that is unpleasant or makes me feel uncomfortable.
- I will tell a teacher or adult I trust if I know of anyone that is behaving badly on line or anyone may be being bullied.

I agree to use IT by these rules when:

- I use school IT or my own in school (including my mobile phone when allowed)
- I use my own IT (including mobile phone) out of school to use school sites or for school activities

I understand that if I break these rules there could be the following consequences:

(1) I might have a sanction in class e.g. missed playtime etc.
(2) I might not be allowed to use the internet or other applications in school.
(3) I might be sent to Mrs Young and my parents called into school.

(4) I could be excluded if I damage things, share inappropriate material, cyber-bully or break the law.

My Name is

My Class teacher is

Signed