ICT Policy

Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. This policy is to be read in conjunction with the following school policies:

- Behaviour and Sanctions Policy
- Safeguarding Children Policies
- Anti-Bullying Policy

The Education and Inspections Act 2006 empowers head teachers 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 online safety incidents covered by this policy, which may take place outside of the school, but are 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.

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 use of ICT that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Headmaster and Senior Leadership Team

- The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Leader of Digital Learning.
- The Headmaster and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headmaster is responsible for ensuring that the Leader of Digital Learning and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Leader of Digital Learning

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.

- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with school technical staff (IT Manager).
- Meets regularly with the Designated Safeguarding Lead to discuss current issues, review incident logs and filtering / change control logs.
- Reports regularly to IT Steering Group.

IT Manager

The IT Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That he keeps up to date with online safety technical information in order to effectively carry out his online safety 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 Headmaster for investigation / action / sanction.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school ICT Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Head teacher / Designated Safeguarding Lead / Leader of Digital Learning for investigation / action / sanction.
- All digital communications with students / pupils / parents / carers are on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the ICT Policy and 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 students / 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.

Designated Safeguarding Lead / Safeguarding Team

The DSL will carry respond to any concerns about online safeguarding/child protection according to the Safeguarding Children Policy. They should be aware of online 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.
- Cyber-bullying.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement.
- 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 online safety practice when using digital technologies out of school and realise that the school's ICT Policy covers their actions out of school, if related to their membership of the school.

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 school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- The school iPads used by their children.
- Their children's personal devices in the school.

Provision of Digital Technology in School

This policy covers the following ICT accounts, services, and hardware/software, as well as any other accounts, services, and hardware/software that staff, students, or members of the school community may use during their day-to-day activities in the school:

Staff

Accounts:

- Microsoft Outlook Email
- MS Teams
- Showbie
- 3sys/PASS MIS
- School Social Media Accounts (Twitter, Facebook, Instagram)

Devices:

- Laptop/Desktop PC
- iPad
- Mobile phone (where appropriate)
- Apple TV (where appropriate)
- Personal mobile phones and e-devices

Pupils

Accounts:

- Microsoft Office 365 (including email)
- MS Teams
- Showbie
- Seesaw
- Century

Devices:

- Access to desktop PCs in ICT suites
- iPad
- Personal mobile phones and other e-devices.

Filtering and Monitoring of Internet Use

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 monitored.).

There is a clear process in place to deal with requests for filtering which is that requests are sent to the Leader of Digital Learning and the ICT Manager and these are logged and actioned after discussion.

The school has provided differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.).

School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

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.

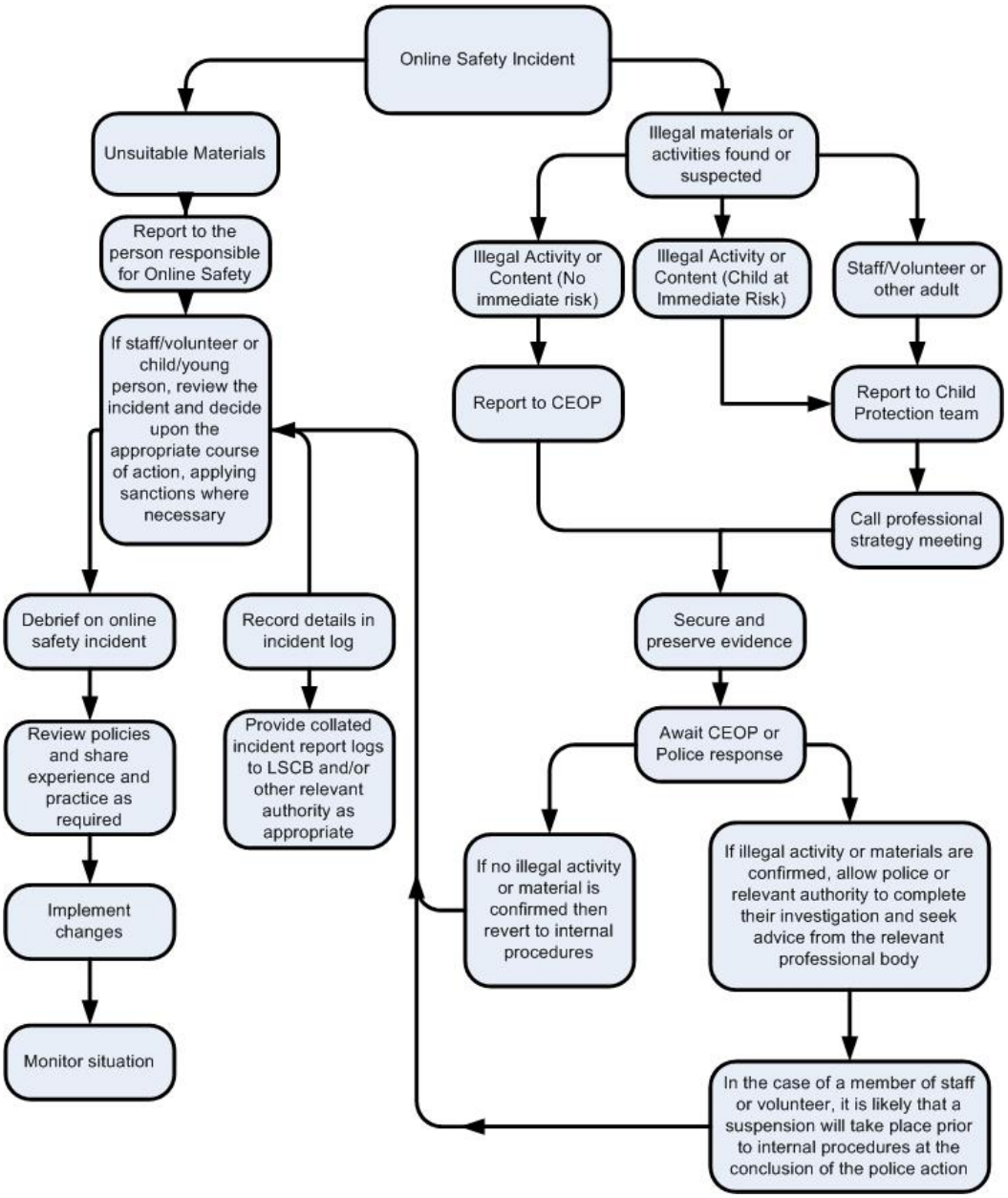
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

Source: used under Creative Commons licencing from South West Grid for Learning exemplar Online Safety policies



Other Incidents

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.
    - 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
    - promotion of terrorism or extremism
    - 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Use of Cameras, Mobile Phones and Personal Electronic Devices in School (Staff and Visitors) Policy

THIS SECTION IS ALSO REPRODUCED WITHIN THE SAFEGUARDING CHILDREN POLICY

This policy follows government legislation and is for the personal protection of staff and visitors.

- Staff may take photographs of children for specific school use only.
- The approved school cameras/iPads must be used.
- Staff should never upload or keep images of school children on their home computer systems.
- Staff should remember that pupils must not take photographs of each other without permission.
- Staff should be aware that some pupils in school must not have their image placed in the public domain, including school web site.
- Staff may have mobile phones or personal electronic devices in school but they must not be used in lesson time.
- Staff working in Pre-Prep with Reception children may not have mobile phones available: they should be locked away. Telephone calls should be made in staff-only areas. It is always suggested that the school landline is used, for their own safety.
- Staff may take a mobile on trips and outings but they are for emergency use only.
- Staff may not make or receive mobile phone calls in teaching time, nor should they leave a lesson to receive or make a call. In extreme circumstances, where a crucial call is expected, staff must let the Headmaster know the situation.
- Staff should not use mobile phones or personal electronic devices to communicate with pupils on social networking sites.
- Visitors should be aware that the use of a mobile phone around school is not allowed.
- Photography by parents and relatives is permitted on the school site; however, it is important that such records remain private and for their own personal use. Such photos and videos must not be sold and must not be put on the internet. Pupils must not be approached or photographed whilst at school, or engaged in activities outside school, without the permission of a member of staff.
- Photographs by other visitors to school are not allowed unless permission has been sought from the Headmaster.

Acceptable Pupil Use of Mobile Phones & Personal E-Devices Policy

Introduction

For young people today the ownership of a personal mobile phone/e-device is considered a vital part of their life. When used creatively and responsibly these have great potential to support a pupil's learning and enhance their life; however, the potential for misuse in school means that clear policy guidelines on use in school is necessary.

These guidelines are intended to help make clear the expectations of the school, for pupil use of mobile phones and e-devices and give clear guidance to staff, pupils and parents about the consequences for misuse.

These guidelines sit alongside the Acceptable Use Policy for ICT, including the use of the school iPads, *which all pupils sign. Pupils will receive age appropriate guidelines and education to help avoid p*otentially dangerous situations, in Digital Learning and LRC lessons. All pupils must look after each other and report concerns of misuse or abuse.

The security of the devices is the pupil's responsibility. It is recommended that all devices are password/PIN protected and that pupils change their password regularly and never reveal it to anyone. The naming of devices is also recommended. Lost/found devices should be taken to Reception.

Rules for Acceptable Use

Who, When and Where?

Pre Prep pupils are not allowed mobile phones. Other pupils are permitted to have a mobile phone in school; however, the following regulations apply:

- Prep School pupils must hand their phone to their class teacher on arrival at school, and may take them back again at the end of the school day.
- Senior School and Sixth Form pupils may carry their phones with them, provided they are used sensibly as below.
- Senior School pupils **MAY** use their phones:
    - In the 6th Form Common Room or library during study periods (6th Form only)
    - During break and lunch times and before/after school in their own day/bag rooms, or next to their iPad locker.
    - Anywhere, anytime, in the case of an urgent need or emergency, with the permission and supervision of a member of staff.
- Senior School pupils **MAY NOT** use or display their phones:
    - In the Dining Room or in Chapel, or during lessons.
    - In the presence of Prep or Pre-Prep pupils
- Boarding houses have rules about handing in of mobile phones in the evenings. See boarding house handbooks.

What and How

- No pupil should have any age-inappropriate material (e.g. videos, games, movies) or bring it into school on any of their electronic devices.
- No pupil should access age-inappropriate material over the internet e.g. YouTube, Netflix and Love Film.
- If asked to do so, pupils must show content on the phone (e.g. messages, emails, pictures, videos, sound files) to a teacher.

Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile phone/e-device and a serious breach of the school's behaviour policy, resulting in sanctions being taken.

- Taking photographic images (still or video) or sound recordings of staff or pupils without their knowledge and explicit permission.
- Photographing or filming in toilets, swimming pools and changing rooms.
- Using a mobile phone or e-device for 'sexting' (the deliberate taking and sending of provocative images or text messages).
- Bullying, harassing, or intimidating staff or pupils by the use of text, e-mail or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites. The School will not tolerate cyberbullying.
- Making disrespectful comments. We expect pupils to treat other pupils and staff online with the same standards of consideration and good manners as they would in a face to face situation.
- Disrupting learning through use of a phone/e-device.
- Refusing to switch off a mobile phone/e-device off or hand it over at the request of a member of staff.
- Using the mobile phone/e device outside school hours or away from school to intimidate or upset staff or pupils: this will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

Dealing with breaches of the Guidelines

The misuse of the mobile phone/e devices will be dealt with using the same principles set out in the school Behaviour and Sanctions Policy, with the response being proportionate to the severity of the misuse. Depending on the nature and severity of the breach, the response may include:

- Asking a pupil to return the phone to the appropriate place, or go to an appropriate place to use it.
- Confiscating the phone.
- Imposing a detention.
- Discussing restrictions to the use of the device with parents.

Heads of School, in consultation with the Deputy Head, will deal with serious incidents of misuse, particularly where there has been a victim of cyberbullying.

Sanctions

Pupils and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines.

The school is within its rights to confiscate or ban a pupil from having a phone/e-device in school, where the guidelines have been breached.

Confiscation procedure

If a mobile phone/e-device is confiscated, the following procedures apply:

- The device may be returned to the pupil at the end of a lesson, at the discretion of the teacher. Alternatively, the pupil will be informed that the device can be collected at the end of the school day from the teacher or, under certain circumstances, Reception/Head of School/House parent.
- The confiscation will be recorded on 3sys, for monitoring purposes.
- The staff member confiscating the device will ensure that confiscated equipment is stored safely, in such a way that it is returned to the correct person.

In the case of repeated misuse the phone/e device will be returned and the pupil will lose the right to bring this sort of device into school, with parents informed.

Serious Misuse or Criminal Activity

Pupils should be aware that the police will be informed if there is a serious misuse where criminal activity is suspected.

If a pupil commits an act which causes serious harassment, alarm or distress to another pupil or member of staff, the ultimate sanction may be permanent exclusion. School will consider the impact on the victim of the act in deciding the sanction and parents will be involved. The Head of School, or Deputy Head will have the right to view files stored in confiscated equipment and will seek the cooperation of parents in deleting any files which are in clear breach of these guidelines unless these are being preserved as evidence. If required, evidence of the offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen. The Head of School will consider whether an incident should be reported to the Safeguarding Team. The Head of School will monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation.

Following any such incident support will be offered and efforts made to facilitate effective closure for the victim. We also ensure that the perpetrator and any others are educated about the impact of their actions. The Head of School will document the case history.

Electronic Devices: Searching and Deletion

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent: authorised staff may search with the pupil's consent for any item.
- Searching without consent: authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

Carrying out the search

- The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
- The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.
- The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.
- The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student/ pupil being searched.

There is a limited exception to this rule: authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search

The person conducting the search may not require the student to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).
The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.
If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible

criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

Confiscation of devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices.

Staff Training

All school staff receive training on online safety and developing digital technology trends annually, and, provided by the Leader of Digital Learning.

Online safety is a core element of safeguarding training. Staff are trained regularly in safeguarding matters, in line with the Safeguarding Children Policy.

Handling of Personal Data

The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected,
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device once it has been transferred or its use is complete.

Reviewed by: Headmaster

Review date: 30 October 2021

Next review: 1 November 2022

Beneath this are agreement/guidelines documents which are also used separately.

ICT Acceptable Use Agreement Pupils

Digital technologies are integral to the lives of children and young people. These technologies are powerful tools which open up new opportunities for everyone. They stimulate discussion, promote creativity and develop awareness of context to promote effective learning. Young people are entitled to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That our pupils will be responsible users and stay safe while using the internet and other digital technologies for both educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils have good access to digital technologies and so enhance their learning and will, in return, expect the pupils to be responsible users.

Acceptable Use Policy Agreement (Pupils)

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission *(see Guidelines for Use of School iPads)*

- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting unless I have permission from a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take any pictures of EYFS pupils.
- I will not take or distribute images of anyone else without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I must follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

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

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the Student Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understood the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school).
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of school for school purposes e.g. communicating with other members of the school, accessing school email, website etc.
- I will not use any e device to bring the school into disrepute.

Name of Student / Pupil	
Group / Class	

Signed

Date

Guidelines for Use of School iPads

The iPad is provided for educational use. You may use it for leisure too but you must ensure nothing interferes with your ability to use it for learning. This includes:

- Leaving enough free memory for school work
- Having it with you at all times for all lessons
- Ensuring the device has enough charge to last a full day of use at school
- Not attempting anything which will breach the software licence agreements (including attempting to 'jailbreak' the device)
- Installing updates to the apps and operating system as directed by the school

Use of the iPad in school is governed by the school's ICT Acceptable Use Policy, and any breach of this policy may result in sanctions.

You are expected to take reasonable precautions to avoid damage to or loss of your iPad. This
includes:

- Not leaving it on view or unattended, for example in a bag or on a car seat
- Always using the protective case supplied by the school at all times
- Only charging the device with an official Apple-approved charger
- Avoiding contact with liquids
- Always knowing where it is, and activating the Find my iPad app
- Using a lock screen wallpaper that contains your name
- Using a pass code
- Never disabling mobile device management

The device is insured but this will not cover carelessness or negligence. You must provide the information needed for a claim to be processed including details of the incident and a police report in the event of a claim for loss/theft.

Any damage to the iPad or its loss, must be reported to the IT Manager immediately. If it accidentally gets wet, do not attempt to turn in on, take it immediately to the IT Manager.

You will be expected to return the iPad when you leave the school.

I have read and agree to abide by the guidelines for school iPad use

Student Name ..... Parent Name .....

Signature ..... Signature .....

Date ..... Date .....

Serial Number .....

Device Name .....