Acceptable Use of ICT Policy

This policy was reviewed in: **January 2026**
This policy is due to be reviewed in: **May 2026**

Contents

General Comments

Pipers Corner School aims to ensure that the latest technologies are used appropriately across the School to enable, enhance and enrich the learning process. Our priority is to provide a reliable network environment to act as a platform for inspirational teaching and efficient administration systems, enabling and supporting our community of learners.

The ICT resources at Pipers are provided for the use of students and staff. They are provided on the understanding that they are not abused, misused or used to offend anyone else, either within or outside the School. They should not be used in a way that will interfere with, disrupt or prevent anyone else legitimately using those resources.

This policy document outlines the acceptable usage expectations to ensure consistency of practice and safe use of the resources. The key principle encompassing this code of conduct is that all users will behave in a responsible way and be considerate to the needs of others.

School-based systems

Classroom guidelines

1. There will be no eating or drinking in teaching areas where there are computers
2. Any student using a school device of any type (e.g. PCs, laptops, iPads and Chromebooks) must have the permission of a member of the teaching staff
3. Once finished using a school device, the user will check that:
    a. They have logged off the system
    b. The computer equipment and the surrounding areas are left tidy
4. There will be no interference in the way the computers and screens are set up
5. Devices borrowed from central storage areas (e.g. chromebooks) must be returned under supervision of a member of staff and put on charge ready for the next user.

Usernames and Passwords

All users of the network will be issued with an individual username and password. This password should be changed by the user. It is the individual's responsibility to remember this password and to keep it secure. All passwords should be at least 8 characters long and ideally should contain at least three of four character types: Upper case letters, lower case letters, numbers and special characters.

Network passwords should be hard to guess and should not be shared with any other online service, such as email, online shopping or streaming services. The use of three random words is one way of creating strong and memorable passwords. We realise this is not practical for our younger students.

No user should log on using someone else's username and password. It is an offence under law to attempt unauthorised access, or to trespass on other users' areas of work.

Staff will be expected to use multi-factor authentication (MFA) where possible to ensure security of access to key school systems (such as email) and data (such as iSAMS). Any device that is used to access school data (whether at home, mobile or at school) must be locked whenever not in use. (On Windows devices use the shortcut Windows Key and L (⊞ -L). Staff should be alert when working in shared family areas or public spaces of the sensitivity of data they are accessing.

Any ICT administrator user account must be used only by the appropriate members of technical and senior staff and exclusively for purposes where privileged access is required. To reduce risk of administrator account compromise, all day-to-day activities of ICT administrative staff will be performed using a non-privileged account.

File storage

Users will be given a **limited** storage area on the onsite server. It is the user's responsibility to delete their unwanted files on a regular basis. Students from Year 3 upwards also have access to cloud

based storage service (as part of the Google Apps suite). Because this is an online system not hosted on our premises the Head of Prep will necessarily need to inform parents of this system each year before new students start using it. Staff also use OneDrive cloud storage to support administration.

No user should use a USB storage device without prior permission from the IT Manager, and files that need to be accessed from a USB device should be checked by IT Support before use.

Printing

Each user of the network will be allocated a print quota and their printing will be monitored. The quota will be sufficient to cover printing requirements during lessons and for coursework. It will not support the unnecessary printing of non-learning material. A charge may be made to students for excessive printing. Staff printing is charged to the department that they are working for. Some staff may be enabled to charge printing to more than one department if appropriate.

We expect that:

1. Users will use print preview facilities to check and amend work before printing
2. Users should consider the need for colour before printing as it is more costly
3. All users should be aware of the environmental impact of the over-use of paper and should print double-sided where possible, or simply share/send the file electronically to the recipient

Software

Pipers Corner School has purchased appropriate software licenses for all programmes installed on the networks. It is against the law to install or use unlicensed programmes on school computers. No programme is to be copied for use on any other computer.

Staff members are not permitted to install programs on their allocated device or any other school owned device. If additional software is required by a member of staff this should be agreed with the IT Team and installed by them.

Subscriptions

Many software resources are available as online subscriptions which can be budgeted for and purchased by IT if budgets are agreed. Any software that requires students and staff to individually login to the system is potentially a Data Protection concern and may need to be entered into the Data Asset Register maintained by the Bursar. All new systems that involved staff or student data must have a Data Impact Assessment completed by the member of staff proposing the use of a new system and approved by the Bursary.

Display screens

Confidentiality is at the heart of these guidelines. The General Data Protection Regulation clearly states that we must protect our data and maintain the privacy of our data subjects (staff and students). Potentially sensitive and confidential data must not be disclosed to any other individual by accident or intention. Please observe the following guidelines.

1. Email, CPOMS or iSAMS should not be used on any device that is currently being displayed on an interactive flat panel or projector or where the device's screen is in view of students.
2. MIS Software should not be used in a classroom except for the purpose of registration, grade entry or entering other information such as sanctions. Viewing student personal details, or editing any document that is sensitive, should only take place in a room where students are not present.
3. Staff should make sure that workstations are either locked (Windows Key and L -L) or logged off if they leave them – even if the machine is in a staff office.

The use of Student Devices

Bring Your Own Device policy (BYOD)

In the Sixth Form we support a BYOD policy whereby students can bring their own device to support their learning. The device is only allowed in school if it has the School's filtering and monitoring software installed to ensure that the device is safe for the students according to Keeping Children Safe in Education guidelines and secure from cybersecurity threats. Students are not permitted to use a device that has not been pre-approved by the IT Team and must not connect to the WIFI without permission.

Some students across all year groups, as identified by the Individual Learning department, are permitted to also bring their own device subject to the same conditions. Unless there are specific requirements, all Individual Learning students will be encouraged to purchased school-managed chromebooks which will then be managed by the IT Department, including filtering and monitoring

Student Devices – Student Expectations

From September 2025, all GCSE students have 1-1 access to student devices.

The expectations are also shared directly with parents.

1. **Availability:** Chromebooks should be brought to every lesson unless the teacher has specifically pre-told the class that they will not be used that day. Each student's allocated device is not to be shared with anyone else.

2. **Charging:** Chromebooks should be fully charged at the beginning of every school day. Students are responsible for ensuring that there is enough charge for each lesson. (In exceptional situations IT Support can provide charging.)

3. **School Usage:** Students must respect the 'traffic light zones' of the School. Red zones mean you must not use the device (e.g. Dining room), orange means you must have staff permission (e.g. classrooms) and green zones means you can choose to use your device.

4. **Behaviour:** Student devices are a privilege, not a right. Any misuse can result losing access. Usage must always be in keeping with the School's Acceptable Use of ICT Policy.

5. **Support:** If the student is aware of a fault in the device, they must report it as soon as possible (break time, lunchtime or after school) to the IT Support office who will get the student and their device working as soon as possible.

6. **Care:** Students must always keep their device in its protective sleeve and ensure they look after it with respect. Any damage resulting from inappropriate care will be charged back to the Parents of the Student.

7. **Home usage:** Students are welcome to connect the device to home Wi-Fi services and printers. However, we ask that students always take care of the device appropriately around the home (e.g. do not eat/drink at the device).

8. **Discernment**: Being allocated a school device does not mean students should use it for every piece of work. Students need to make good judgements about their use of technology as guided by their teachers.

9. **Wellbeing**: It is good practice to not use screens for at least 1 hour before going to bed. Take regular breaks from the screen and students should manage their homework so that Chromebooks are switched off early enough to enable good quality sleep.

10. **Responsibility:** The provision of the Chromebook does not take away the ongoing family discussion about online safety. Whilst school filtering and monitoring software will be active on the School devices, parents remain responsible for their child's internet use in the home.

The Use of Mobile Phones by Students

For many young people today the ownership of a mobile phone is considered a necessary and vital part of their social life. When used creatively and responsibly the smart phone has great potential to support a student's learning experiences (e.g. managing Google Classroom tasks or accessing learning resources). The school has, however, had occasional incidents of poor conduct where mobile phone misuse has been a feature. This has been particularly difficult to address when mobile technologies are an element. Bullying, intimidation and harassment are not new in society; however, bullying using a mobile phone represents an ongoing challenge for all schools to manage. Parents and students should be clear that misuse of mobile phones and equivalent technologies will not be tolerated.

Smart phones include many functions that have the potential for misuse such as high-quality cameras, instant messaging, GPS tracking and mobile access to the internet. These allow easy multimedia creation and immediate sharing on messaging and social networking sites such as WhatsApp, Snapchat and Instagram. Basic mobile phones are available cheaply (e.g. Nokia 105) that do not have any of the 'smart' features listed above and these are known as 'basic' phones. Basic phones are acceptable for our younger students to bring in as long as students abide by this policy.

For clarity, any device that has any of the smart features outlined above (this includes tablets, watches, glasses or other wearable technologies) are considered equivalent to smart phones within this policy and are therefore subject to the same restrictions. This is especially pertinent for devices (e.g. some watches and laptops) that have built-in 4g/5g internet connectivity.

Acceptable Use of a Mobile Phone in School by Students

Students do not need to bring in any mobile phones to engage in their educational activities within the school. Students are allowed to bring in mobile phones but **all student mobile phones should be switched off from the moment that they come through the school gate**. If students choose to bring in a mobile phone of any type it is on the understanding that they agree with the following limitations on its use, namely:

Students in Years 3 to 6 are not permitted to bring in smart phones. They can only bring in a basic phone if they are travelling on the school coaches. Prep students who travel on school coaches and choose to bring in a basic phone must hand it in to the Prep Office on arrival at school.

Students in Years 7 to 9 are not permitted to have smart phones on the school site and must hand in their basic phones to the School Office on arrival at school.

Students in Year 10 are required to hand their phones in to the School Office on arrival at school.

Students in Years 11 are allowed to have mobile phones in school on the following conditions:

- Mobile phones must be switched off from the moment that they come through the school gate and remain off whilst students are on the School premises. This includes break and lunchtimes. It is not acceptable for phones merely to be put on silent or pager mode.
- The phone must be kept out of sight during lessons. If staff are leading an educational activity where students' access to mobile phones in lessons could be useful, this must have been pre-approved by the Senior Leadership Team.
- No student may take a mobile phone into a room or other area where examinations are being held.
- The security of the phone will remain the student's responsibility at all times including PE/gym lessons.
- If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher.

Students in Years 12 & 13 are allowed to have mobile phones in school on the following conditions:

- Mobile phones must only be used in the Sixth Form Centre – they should not be used anywhere else in School other than as highlighted below.
- The phone must be kept out of sight during lessons. If staff are leading an educational activity where students' access to mobile phones in lessons could be useful, this must have been pre-approved by the Senior Leadership Team.
- No student may take a mobile phone into a room or other area where examinations are being held.
- The security of the phone will remain the student's responsibility at all times including PE/gym lessons.
- If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher.
- The phone must not be connected to the School Wi-Fi.
- Students should not be using a mobile phone while still on School property outside of the Sixth Form Centre.

Unacceptable Use of Mobile Phones

The following are examples of misuse but are not exclusive. "Misuse" will be at the discretion of the Headmistress:

- The deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience such as on Snapchat, YouTube or TikTok
- The use of a mobile phone for Youth Produced Sexual Imagery ("sexting"). i.e. The deliberate taking and sending of provocative images or text messages
- Students posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm to others
- Making disrespectful comments, misrepresenting events or making defamatory remarks about teachers or other students
- General disruption to learning caused by students accessing phones in lessons
- Students phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised
- Publishing photographs of vulnerable students, who may be on a child protection plan, where this may put them at additional risk

The School will consider any of the following to be unacceptable use of the mobile phone and a serious breach of the School's Behaviour policy resulting in sanctions being taken.

- Photographing or filming staff or other students without their knowledge or permission
- Photographing or filming in toilets, changing rooms and similar areas
- Bullying, harassing or intimidating staff or students by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites
- Refusing to switch a phone off or handing over the phone at the request of a member of staff
- Using the mobile phone outside school hours to intimidate or upset staff or students will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.
- Using a mobile phone outside school hours in such a way that it undermines the stability of the School and compromises its ability to fulfil the stated aim of providing "a clear moral and ethical lead".

Dealing with breaches

Misuse of the mobile phone will be dealt with using the same principles set out in the School Behaviour policy, with the response being proportionate to the severity of the misuse. Students are

aware that serious misuse may lead to the confiscation of their mobile phone, communication with parents and the imposition of other sanctions up to and including exclusion from school. If the offence is serious it will be reported to the Police.

Where it is deemed necessary to examine the contents of a mobile phone this will be done by a designated member of staff. The action will be properly recorded in case it later becomes evidence of criminal activity. The record will include the time, who was present and what is found.

Confiscation procedure

- If a mobile phone is confiscated it will be kept securely, and the School will ensure that confiscated equipment is stored in such a way that it is returned to the correct person
- The confiscation will be recorded in the School behaviour log for monitoring purposes. Where a student persistently breaches the expectations, following a clear warning, the Headmistress may impose an outright ban from bringing a mobile phone into school. This may be a fixed period or a permanent ban.
- In the case of repeated or serious misuse the phone will only be returned to a parent/carer who will be required to visit the School by appointment to collect the phone. At the discretion of the Headmistress the phone may be returned to the student at the end of the confiscation period

Mobile Phone Sanctions

Students and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines, following the School's Rewards, Behaviour and Sanctions policy. Students and their parents should be very clear that the School is within its rights to confiscate the phone where the guidelines have been breached.

Using the mobile phone outside school hours to intimidate or upset staff or students or undermine the stability of the School in any way will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

- Any misuse of the mobile phone by students the phone may be confiscated for one week for the first offence and up to one month for the second offence depending on the offence. If a phone is confiscated, school will make it clear for how long this will be and the procedure for its return.
- Students should be aware that the police will be informed if there is a serious misuse of the mobile phone where criminal activity is suspected.
- If a student commits an act which causes serious harassment, alarm or distress to another student 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.

Where the phone has been used for an unacceptable purpose

- The Headmistress or a designated staff member will have the right to view files stored in confiscated equipment and if necessary seek the cooperation of parents in deleting any files which are in clear breach of these guidelines unless they are being preserved as evidence.
- If required evidence of the offence or suspected offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen.
- The DSL may need to refer a serious incident to external agencies
- The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation

Internet systems

It is our School policy, as an element of safeguarding and our duty of care, to continuously monitor our internal network and external systems for any inappropriate use. The internet is provided to

support the core tasks of teaching, learning and school administration. Other uses during school hours are not permitted.

Web filtering

Filtered internet access is provided for all users at Pipers Corner School. For some categories of websites (e.g. shopping) the filter allows users to 'click through' to gain access to the website. If you do choose to click through the filter please remember that all web usage is monitored and you are responsible for ensuring that the websites you are visiting are appropriate and relate directly to the work that you are doing. Filtering logs for all users are automatically stored for 30 days.

We expect that users will:
1. Not waste time and resources by accessing trivial or time-wasting material
2. Not deliberately access illegal or offensive material

The School will:
1. Ensure that students are provided with the necessary skills to encourage appropriate use
2. Review the Internet access log as necessary should misuse be suspected
3. Register any unsuitable site on our filter and deny access immediately

A filter report is produced and checked on a daily basis to monitor internet searches and sites accessed.

Device Monitoring

The School also uses software which automatically monitors the School IT system (for example, it would raise an alert if a user visited a blocked website or sent an email containing an inappropriate word or phrase). All school devices (and some cloud systems) that are used by users have monitoring technology installed to detect user misuse or safeguarding concerns. Behaviour that is deemed to fall into one of the following categories will be automatically flagged to senior members of our safeguarding committee who will investigate and respond as necessary:

- Cyberbullying and offensive behaviours
- Online criminality
- Inappropriate sexual behaviour
- Oversharing of personal data
- Extremism or terrorist grooming
- Vulnerable persons

Please note: This service is always active on chromebooks and Google Chrome browsers that are logged in to a school account regardless of location.

If anything of concern is revealed as a result of the monitoring service then this information will be shared with key members of the School's safeguarding team and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police. Our use of filtering and monitoring technology ensures we fulfil the expectations set out in the statutory document Keeping Children Safe in Education.

Email

All users are issued with email accounts of the format *[username]@piperscorner.co.uk* accessible via Microsoft Outlook. Email accounts are to be used for educational purposes and not for personal use. Students and staff are also issued with Google accounts as part of the Google Apps suite.

Anything that is written in an email or other technology-based communication is treated in the same way as any form of writing. You should not include anything in an email or technology-based communication which is not appropriate to be published generally. Any email message or other technology-based communication which is abusive, discriminatory or defamatory is not permitted. Use of the email system in this way constitutes a breach of the School's Bullying policy and may constitute gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

We expect that:

1. No user will send illegal, offensive or defamatory messages
2. No user will send material that is designed, or is likely, to cause annoyance, inconvenience or distress. This kind of use can become cyber-bullying
3. No user will send or redirect chain letters
4. Email should only be used during a lesson if it is directly related to the learning activity
5. Emails should always be professional in manner and content as they can be legally requested in certain circumstances. Reply to all should be used with care.

You should be aware that emails, texts and other messages are disclosable as evidence in court proceedings. This is the case regardless of whether the communication has taken place using the School's equipment and systems, or your own equipment and social media/messaging service. Even if messages are deleted, a copy may exist on a back-up system or other storage area.

Malware and Cybersecurity

Malware (e.g. viruses and ransomware) can quickly disrupt and in some cases disable computer systems. The School runs active security software on all its computer systems. Malware commonly activates when users open email attachments or untrustworthy websites. No email attachment should be opened and no website should be visited unless the source is reasonably considered to be trustworthy. Any unusual emails or device behaviour should be reported immediately to IT.

Copyright

Copyright refers to the rights that protect the works of authors and other creative people against copying or unauthorised public use. Copyright generally covers original works of literary, dramatic, musical or artistic expression. Copyright laws do extend to the Internet, although UK legislation allows for certain permissions to cover educational use. Users may make limited use of copyright materials in their work, but acknowledgments must be made. This can be achieved by including the full Web address of the page where the information was found.

Teachers will monitor work with these issues in mind and advise students where appropriate.

Video Conferencing

The School may use video conferencing tools to support the education of students. In addition to mobile devices there are some classrooms that are set up with enhanced hardware (e.g. Harkness and the Library classroom). In some circumstances (pre-agreed with the Senior Leadership Team) video-conferencing can be used between students and staff whilst they are working at home (for example in an extended period of time whereby staff or students cannot access the School site). Video conferences involving students should only be conducted using agreed school platforms (currently Google Meet) and should adhere to the following guidelines.

For the member of staff hosting a video conference:

1. **Every meeting involving students should have a unique meeting code**
   If the code was shared, accidentally or purposefully, the safety of the classroom is compromised.
2. **Use the Waiting Room function**
   This is an essential way of checking who is coming into the video conferencing room
3. **"Join before host" must be set to OFF**
   Do not let students enter the VC room before the host member of staff
4. **Hosts should familiarise themselves with security functionality**
   Functions staff may use include not allowing students to share their screen or use chat

When attending a video conference all users (staff and students) must behave as if you are at school even if you are working remotely:

1. Choose a professional location if possible (e.g. dining room)
2. Look professional (mufti day guidelines for students)
3. Warn other members of your household or department to avoid interruptions

4. Have screens turned on to demonstrate engagement with the meeting or lesson
5. Use your name in the VC software so others in the meeting know who you are

Further guidance is available: https://piperscornerschool.sharepoint.com/sites/StudentITSupport/SitePages/Video-Conferencing-for-Lea.aspx

Artificial intelligence

The School has a separate policy on Artificial Intelligence that is based on the principles:

1. Artificial Intelligence is neither a good or bad technology, but its application can be either
2. Students have the potential to use AI to enhance their learning
3. Students' academic integrity is compromised if AI generated work is submitted as their own
4. Teachers have the potential to use AI to reduce their workload
5. AI is an imperfect technology

Misuse of Artificial Intelligence is clearly explained in JCQ guidelines and JCQ guidelines are published in all Senior School departmental areas. The need to maintain Academic Integrity is also reflected in the School's Rewards and Sanctions behaviour matrix.

Positive use of Artificial Intelligence is taught to Year 10 students as part of the Academic Literacy curriculum and to Year 12 students as part of the Enrichment curriculum. All staff are encouraged to use AI positively both in teaching and administrative activities.

VPN

Safety and Safeguarding Risks
The primary reason schools block VPNs is to fulfil their **duty of care**. Schools use web filters to prevent students from seeing harmful content, such as graphic violence, adult material, or extremist websites. A VPN creates an encrypted "tunnel" that makes your traffic invisible to the school's filter. This means you could accidentally (or intentionally) access dangerous sites that the school is legally required to block. If a student is being bullied or groomed online, school monitoring systems can often flag suspicious keywords or activity to alert staff.
A VPN hides this activity, making it impossible for the school to intervene and protect the student.

Students often turn to **free VPNs**, to enable them to bypass Country specific security, for example viewing specific media content or worse, accessing websites that require age verification in some countries. Many free VPN apps monetize by injecting ads or, worse, installing malware and trackers on a device. A VPN can act as a bridge for hackers to enter the school's private network, potentially compromising the data of thousands of other students and teachers.

VPNs interfere with the balance of the School's network performance.
VPNs add extra layers of encryption and route data through distant servers. This slows down the connection and can lag the entire school Wi-Fi for everyone else. Many educational tools (like library databases or testing software) are configured to work only within the school's "clean" network. Using a VPN can break these connections, making it impossible to submit assignments or access research.

As a result, the use of a VPN by Students and Staff is strictly prohibited

Key Staff

Digital Learning

There is a Digital Learning team of teachers representing all age groups and academic disciplines that meets regularly to develop the technology usage within teaching and learning activities. This team is coordinated by Mr Alex Rees.

IT Support

Technical concerns about IT can be reported to IT Support team on support@piperscorner.co.uk where the team will respond appropriately. This team is managed by Mr Andrew Bryson.

Online safety in School

The Designated Safeguarding Lead (DSL) is responsible for all safeguarding. The DSL is Mr Andrew McClean, deputised by Mrs Helen Ness-Gifford and Mrs Caroline Derbyshire, supported by the Safeguarding Committee. The Assistant Head, Digital Learning, Mr Alex Rees, is part of the Safeguarding Committee to support the DSLs as required with regard to online safety.

If any member of the School community has a safeguarding concern, regardless as to whether it involves technology or not, you should report it to the DSL or the Deputy DSLs as normal.

Education provision for students, building the students' resilience to online risks, and including a wide range of eSafety issues is provided for within the Life Skills and the ICT curriculum areas managed by Mrs Rachael Coe and Miss Lou Scott respectively. This is supported by outside speakers.

Education provision for parents is provided regularly by Mrs Helen Ness-Gifford who speaks to parents at Parents Evenings about the risks associated with social media at different ages. This is supported by relevant speakers invited to present as part of the Parent Partnership Programme and occasional directed emails to parents of specific year groups when a specific risk has been identified as relevant for our students.

Education for staff is provided as part of the Staff Induction process managed by Mr Alex Rees, Assistant Head, Digital Learning, when new staff are introduced to this document and asked to sign it. IT related training for staff is provided as part of the INSET schedule and all training reinforces the School Acceptable Use policy where relevant. On a biennial basis all staff complete Online Safety training and receive updates in the intervening years.

Online Safety outside School

The School's filtering and monitoring services can be activated on non-school devices outside school when a school username is logged in. The School will always respond in a timely manner within school hours to flagged alerts from these systems. Parents are always directly responsible for their child's online behaviour outside school hours and it is recommended that families install appropriate filtering and monitoring systems on student devices not directly managed by the School.

Students should at no time use social media or any other systems to make comments to or about other members of the School community that constitute bullying of any kind and should take care not to write anything that could be interpreted as bullying even if not intended to be so. Any reports of such behaviour, evidenced by screenshots or downloads, will be investigated thoroughly and may lead to sanctions under the Rewards and Sanctions Policy.

The School reserves the right to make random checks of students' devices to ensure that they are not using inappropriate language or being unkind online. This is part of the students' education and we anticipate parents will engage in similar checks at home to complement the in-school approach.

Agreement for Staff

The School will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users. This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems, and the data stored on them, are protected from accidental or deliberate misuse.

General Principles

- ☑ I will uphold this Acceptable use of ICT policy when using school systems, whether in-school or at home, aware of the core principle that all users will behave in a responsible way and be considerate to the needs of others.
- ☑ 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.
- ☑ I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work.
- ☑ When I use a personal device (e.g. mobile phone) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date software and are free from malware.
- ☑ I will immediately report any damage or faults involving school equipment or software, and concerns about the potential misuse of technology, however this may have happened.
- ☑ I will not plug in a non-school device to a school device or the school network (Examples are in Appendix 5)

To ensure my professional and personal safety

- ☑ I understand that the School uses filtering and monitoring software in keeping with the statutory Keeping Children Safe in Education guidelines. These systems filter and monitor my use of school ICT systems, email and other digital communications, including searches undertaken using the School's internet service.
- ☑ I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
- ☑ I will ensure that when I take and / or publish images of others I will do so with their permission and only in accordance with the School's policy on the use of digital / video images.
- ☑ I will only communicate with students and parents / carers using official school systems and not via personal email accounts or other communications (e.g. Facebook, WhatsApp). All communication will be professional in tone and manner.
- ☑ I will not engage in any on-line activity (either in or outside school) that may compromise my professional responsibilities or the reputation of the School.

- ☑ I will be professional in my use of all school systems (especially email, CPOMS and iSAMS).

To maintain data protection

- ☑ Potentially sensitive and confidential data may be contained in emails/MIS/CPOMS within school and must not be disclosed to any other individual by accident or intention.
- ☑ I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy. If I access school systems (such as email) from personal devices then I will ensure the device is password protected with a timed lock.
- ☑ Where personal data (other than data need in the course of teaching, e.g. marks, grades etc.) is transferred outside the secure school network, it must be encrypted.
- ☑ No USB keys or USB hard disks can be used on site unless they are provided by IT Support. Personal USB storage systems are not permitted, but instead staff may use school managed cloud storage systems to work on files when off the School site.
- ☑ I will not use a personal device (e.g. tablet or laptop) for school work regularly. (The IT team will supply a school mobile device for all staff whose job role requires it.) When I use a personal device for doing school work (e.g. at home) I will not synchronise school data onto my personal device, but work with school files directly in the M365 cloud where possible.
- ☑ The School supports the use of specific apps on personal mobile phones (such as Outlook) which temporarily store school data in encrypted format and utilise multi-factor authentication (MFA) as long as the phone is not shared with other family members.

Summary statements:

- ☑ I understand that this Acceptable Use Policy applies not only to my work and use of ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the School.
- ☑ I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, and in the event of illegal activities the involvement of the police.
- ☑ I have read and understand the above and agree to use the School ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the School) within these guidelines.
- ☑ Any equipment the School allocates directly to me to support my role (e.g. laptop, iPad, ...) must be returned to the School on request at any time in full working order together with associated power cables and peripherals. Any damage or loss of school property must be reported as soon as I become aware of it and I understand that I may be charged for the repair or replacement of the School equipment.

Staff / Volunteer Name:	
Signed:	Date:

The School will request that this policy document is reviewed and re-signed regularly during my period of employment.

Acceptable Use of ICT Agreement for Students in Senior School

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 ICT systems, email and other digital communications.
- ☑ I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- ☑ 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.
- ☑ 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 pictures and text that I upload to online services (such as Snapchat, Instagram and WhatsApp) is easy for recipients to copy and potentially misuse without my knowledge. It is not always possible to remove such data once it is posted.

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 or distribute images of anyone or make audio or visual recordings without their permission.
- ☑ I will be held personally responsible for all data I have placed on a website or electronically communicated to others. Material of a threatening, abusive, bullying, racist, harassing or defamatory nature, whether placed or sent during or outside school time (including the holidays) will be treated as a serious breach of the School discipline code.
- ☑ I will report any misuse of networking websites which has been undertaken by a member of the School. This may be done on a "no-names" basis provided sufficient information is given to enable the School to take action.

Protecting school technology:

- ☑ 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 programs 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 attachment to emails, or follow links embedded within emails, unless I know and trust the person that sent the email, due to the risk of viruses or other harmful programs.
- ☑ I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- ☑ I will only use AI services and social networking systems in school time with staff permission, in keeping with the service's terms and conditions, especially mindful of age restrictions.
- ☑ I will not use email during lessons unless I have permission from the teacher to do so.

- ☑ No USB keys or USB hard disks can be used on site unless they are provided by IT Support. Personal USB storage systems are not permitted, but instead I will use school managed cloud storage systems (e.g. Google Drive) to access and work on files when off the School site.
- ☑ If I have been given permission to use my personal devices (laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from malware.

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

- ☑ I must make full and accurate references to all work from others, including AI services, that I use in my studies. This applies to sources on the internet as well as paper based sources such as books. Where appropriate I should seek permission to use the original work of others.
- ☑ Where work is protected by copyright, I will not try to download copies (including music and videos from YouTube).
- ☑ When I am using the internet and AI services to research information, I should take care to check that the information that I access is accurate and free from bias. I understand that external sources may not be truthful and can occasionally purposefully 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 the school name and logo are protected by copyright. I will not use the School name or logo in any websites, blogs, social media posts, etc. that I create, in a way that could be misinterpreted as having been approved by the School.
- ☑ I understand that the School's policy is that complaints, gossip or rumour about the School or a member of the School community will be investigated. Where they relate to the use of websites, the School reserves the right to use inspection software to view web pages. This right will only be exercised when considered by the Headmistress to be necessary and reasonable. In each case a decision to view web pages will be balanced against the student's right to respect for private and family life.
- ☑ I understand that the School may use anti-plagiarism software to check that work I submit is my own. I am aware that AI work submitted as if it is my own is a type of plagiarism.
- ☑ I should not sign up for online services that are not permitted for my age. I must not lie online (e.g. altering my date of birth) in order to gain access to an online service (e.g. WhatsApp) purposefully contravening the terms and conditions of that service.

Summary statements:

- ☑ I understand that this Acceptable Use Policy applies not only to my use of ICT equipment in school, but also applies to my use of school ICT accounts, systems and equipment out of school and my use of personal equipment in school or in situations related to my education.
- ☑ I have read and understand the above and agree to use the School ICT systems (both in and out of school) and my own within these guidelines.
- ☑ I will uphold the Acceptable Use of ICT Policy, aware of the core principle that all users will behave in a responsible way and be considerate to the needs of others.
- ☑ 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.
- ☑

Student Name:	
Signed:	Date:

The School will request that this policy document is reviewed and re-signed regularly during my school career.

Acceptable Use of ICT Agreement for Students in Pre-Prep and Prep

At Pipers we make use of digital technology to enhance the learning experience of our pupils. From Year 2 this includes the Google Suite, which is used to complete assignments, communicate with teachers, and learn 21st century digital citizenship skills. The School requires your permission to provide and manage a Google account, which will then fall under the terms of our school acceptable use ICT agreement. We have successfully used the Google Suite over many years, and I am sure you are familiar with Google as a company. If you do have any questions, please let your form tutor know.

Acceptable Use Principles:

- ❑ I will treat my username like my toothbrush – I will not share it, and I will not try to use any other person's username and password.
- ❑ I will not share personal information about myself or others when on-line.
- ❑ I will tell an adult about anything that I see on a computer that makes me feel uncomfortable.
- ❑ I will be polite when I communicate with others.
- ❑ I will not take photos, audio or video of anyone without their permission.
- ❑ I will not sign up for any online services which are not designed for my age-group (and then only with the permission of my teacher or parent).
- ❑ I will not lie online (for example, about my age).
- ❑ I will report any problem that I notice with school computers, however this may have happened.

Student Name:	
I can confirm that I have read through this code of conduct with the above-named student and that they have understood the above rules for the use of IT in school. I can confirm that I agree to Pipers Corner School creating and managing a Google Workspace for Education account for my child (Year 2 and above only).	
Parent name:	
Signed:	Date:

The School will request that this policy document is reviewed and re-signed regularly during my school career

Appendix One - Guidance on Confiscation of Devices

Department for Education guide on screening and searching – What the law allows

- Schools can require students to undergo screening by a walk-through or hand-held metal detector (arch or wand) even if they do not suspect them of having a weapon and without the consent of the students
- Schools' statutory power to make rules on student behaviour and their duty as an employer to manage the safety of staff, students and visitors enables them to impose a requirement that students undergo screening
- Any member of school staff can screen students

Please see link for the full document:

Searching, screening and confiscation (Guidance Updated July 2023)
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Appendix Two - Legal Context

Common Offences Related to the Misuse of Mobile Phones

The key to both offences below is that the message/picture/video is actually SENT. (If it is only stored on a device the offence is not complete.)

Malicious Communications Act 2003

It is an offence to send an indecent, grossly offensive or threatening letter, electronic communication or other article to another person with the intention that it should cause them distress or anxiety.

Communications Act 2003
Section 127 covers all forms of public communications

1. **A person is guilty of an offence if they**

a) send by means of public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character or
b) causes any such message or matter to be sent.

2. **A person is guilty of an offence if, for the purposes of causing annoyance, inconvenience or needless anxiety to another they**

a) send by means of a public electronic communications network, a message that they know to be false,
b) causes such a message to be sent or
c) persistently makes use of a public electronic communications network by confiscation of the device and keeping it secure or by taking photographs of the screen

Appendix Three - Police response to an incident in School

Extract from the Home Office guidance on the action police should take if a crime may have occurred in school.

In order to sustain the disciplinary authority of schools, this guidance clarifies the general principles of NCRS as they apply specifically to incidents on school premises. When police have reported to them an incident which took place on school premises, including those witnessed by, or reported directly to, offices working in the School, which they would normally record as a notifiable offence will, in the first instance, invite the victim or the person acting on their behalf to report the matter to the head teacher to be dealt with under normal school discipline procedures. Such reports should be recorded as an incident only, until or unless:

a) they judge it to be a serious incident as defined below; (see full document)
b) having brought the matter to the attention of the School in line with good practice (see references to guidance papers below), they receive a formal request from the School to create a crime record; or
c) the child, parent or guardian or the child's representative asks the police to create a crime record.

For full descriptions see Annex B: Crime Recording (Schools Protocol)

Appendix Four - Sources of help

Resources

Resources are available to support teachers, parents and students to promote the safe use of mobile phones and other technologies both in school and at home. Below is a note of the resources available and a short description of what each one contains. These resources have been drawn from a variety of sources, including the Mobile Network Organisations.

- Ofcom, the regulator for communications services, has published useful information on unwanted calls and messages on their website at: https://www.ofcom.org.uk/phones-and-broadband/unwanted-calls-and-messages/tackling-nuisance-calls-and-messages

For students

- The National Bullying Helpline offers advice on their website at: https://www.nationalbullyinghelpline.co.uk/cyberbullying.html

- **Childline** https://www.childline.org.uk/

- **Child Exploitation and Online Protection Centre** https://www.ceop.police.uk/Safety-Centre/

Appendix Five – Devices that should not be attached to the school network

To protect a school network, the general rule is: **If the school didn't buy it, don't plug it in.** School networks are high-value targets for ransomware and data breaches. Plugging in an unauthorised device can bypass firewalls, introduce malware, or create "shadow IT" (unmanaged equipment) that the IT team cannot protect.

The following list of devices are prohibited from being plugged into school devices or directly into the network itself without the express permission of the IT Team. This list is by no means exhaustive but gives a general idea of what is not allowed.

Removable Storage

- USB Flash Drives / Thumb Drives
- External Hard Drives & SSDs
- SD Cards

Personal Communication & Mobile Devices - while these are often used for charging, a USB cable also acts as a **data bridge**.

- Personal Smartphones & Tablets
- Smartwatches

Personal Peripheral Equipment

- Personal Keyboards & Mice
- Unbranded USB Hubs
- USB "Fans" or "Lights"

Internet of Things (IoT) & "Smart" Gadgets are devices that "talk" to the internet without a screen are often the least secure.

- Voice Assistants (Alexa/Google Home
- Gaming Consoles
- Smart Toys

Mini switches and hubs (often called "unmanaged switches") are particularly dangerous for school networks. While they seem like a harmless way to get more sockets under a desk, they can cause serious problems on the School network