



# E-Safety and Acceptable Use of ICT Policy

Version 1.5 | September 2025

**First Implementation date** | September 2019

**Review period** | Annually

**Date last reviewed** | September 2025

**Document reference** | PL1.6

**Responsible person** | Zoe Woolley and Joanna Singleton

## 1.0 Introduction

Knowledge Gate International School aims to ensure that every student in its care is safe, and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose more significant and more subtle risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music/video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smartphones and tablets.

This policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

While exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies. We understand the responsibility to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the School IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Agreements cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smartphones, etc.).

## **2.0 Roles & Responsibilities**

### **2.1 The School Board**

The School Board is responsible for the approval of this policy and for reviewing its effectiveness. The School Board will review this policy at least annually.

### **2.2 Executive Principal and the School Leadership Team**

The Executive Principal is responsible for the safety of the members of the school community, and this includes responsibility for e-safety. The Executive Principal has delegated day-to-day responsibility to the e-safety coordinator and Designated Safeguarding Lead (DSL). In particular, the role of the Executive Principal and the School Leadership Team is to ensure that staff, in particular, the e-safety coordinator, are adequately trained about e-safety and are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

### **2.3 E-safety Coordinator**

The School's e-safety coordinator is responsible to the Executive Principal for the day to day issues relating to e-safety. The e-safety coordinator has responsibility for ensuring this policy is upheld by all members of the school community and works with IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations.

### **2.4 IT staff**

The School's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate use to the e-safety coordinator and Executive Principal.

### **2.5 Teaching and support staff**

All staff are required to sign the Staff Acceptable Use Agreement before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture to address any e-safety issues which may arise in classrooms on a daily basis.

### **2.6 Students**

Students are responsible for using the school IT systems following the Acceptable Use Agreement, and for letting staff know if they see IT systems being misused.

### **2.7 Parents and Carers**

The school believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The School will always contact parents if it has any concerns about students' behaviour in this area and likewise, it hopes that parents will feel able to share any concerns with the School.

Parents and carers are responsible for endorsing the School's Student Acceptable Use Agreement.

### **3.0 Education and Training**

#### **3.1 Staff: awareness and training**

New teaching staff receive information on e-Safety and Acceptable Use Agreements as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of CPD training and internal meeting time, and are made aware of their responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff receive information about e-safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. These behaviours are summarised in the Acceptable Use Agreement, which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be sent by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's e-Safety Coordinator and DSL. The School's DSL keeps a log of any reported incidents, including in the student's file where it pertains to an individual.

#### **3.2 Students: e-Safety in the curriculum**

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to students on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our students' understanding of it.

The School provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually, via PSHE, students are taught about their e-safety responsibilities and to look after their online safety. From Grade 1, students formally in lessons are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their

duty to report any such instances they or their peers come across. Students can report concerns to the Designated Safeguarding Lead and the e-Safety Coordinator or any member of staff at the school who will report concerns to the relevant person.

From Grade 6 they are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Students are taught about respecting other people's information and images through discussion and classroom activities.

Students should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Students should approach the Designated Safeguarding Lead, the School Counsellor or the e-Safety Coordinator as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

### **3.3 Parents**

The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents if it has any concerns about students' behaviour in this area and likewise, it hopes that parents will feel able to share any concerns with the School.

The School recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The school therefore arranges annual discussion evenings for parents when an outside specialist gives advice about e-safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. Videos of the presentation and the accompanying documentation are sent to new parents and available on request.

## **4.0 Use of school and personal devices**

### **4.1 Staff**

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device that is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are referred to the Staff Code of Conduct for further guidance on the use of non-school owned electronic devices for work purposes.

Staff are permitted to bring in personal devices for their use. They may use such devices during break-times and lunchtimes.

Staff working in the early years should note that personal devices **MUST** be left in the School Office or the staffroom, they are not permitted to be used anywhere in early years areas outside of the school office or staff room.

Personal telephone numbers, email addresses, or other contact details may not be shared with students or parents/carers and under no circumstances may staff contact a student or parent/carers

using a personal telephone number, email address, social media, or other messaging systems.

#### 4.2 Students

If students in Grades 6 to 12 bring in mobile devices (e.g. for use during the journey to and from school), they should be kept switched off and out of sight all day, and will remain the responsibility of the child in case of loss or damage. In the exceptional cases of Primary students bringing in a Mobile Device, these must be handed in to the Homeroom Teacher at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The School has introduced the use of student-owned tablets/laptops as a teaching and learning tool, and students are required to adhere to the BYOD Policy when using tablets for schoolwork. In particular, the Student BYOD Policy requires students to ensure that their use of tablets/laptops for schoolwork complies with this policy and the Student Acceptable Use Policy and prohibits students from using tablets/laptops for non-school related activities during the school day.

The School recognises that mobile devices are sometimes used by students for medical purposes or as an adjustment to assist students who have disabilities or special educational needs. Where a student needs to use a mobile device for such purposes, the student's parents or carers should arrange a meeting with the Head of School to agree how the school can appropriately support such use. The student's teachers and other relevant members of staff will be informed about how the student will use the device at school.

### 5.0 Use of internet and email

#### 5.1 Staff

Staff must not access social networking sites, personal email or any website or personal email which is unconnected with school work or business from school devices or while teaching / in front of students. Such access may only be made from staff members' own devices while in staff-only areas of the School.

When accessed from staff members' devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The School has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the e-Safety Coordinator / IT Manager, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to the e- Safety Coordinator / IT Manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring the school into disrepute;

- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school students or parents be added to social network 'friends' or contacted through social media.

Any digital communication between staff and students or parents/carers must be professional in tone and content. Under no circumstances may staff contact a student or parent/carer using any personal email address or telephone number. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

## 5.2 Students

All students are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all schoolwork. Students should be aware that email communications through the school network and school email addresses are monitored.

There is strong antivirus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, students should contact the IT team for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the e-Safety Coordinator / IT Manager / or another member of staff.

The school expects students to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Students must report any accidental access to materials of a violent or sexual nature directly to the e-Safety Coordinator / IT Manager / or another member of staff. Deliberate access to any inappropriate materials by a student will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Policy. Students should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work/research purposes, students should contact the IT team for assistance.

## **6.0 Course of action if inappropriate content is found**

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
  - Turn off the monitor or minimise the window.
  - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
  - Ensure the well-being of the student.
  - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the students).
  - Report the details of the incident to the e-Safety Co-ordinator.
- The e-Safety Co-ordinator will then:
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

## **7.0 Data storage and processing**

The School takes its compliance with the General Data Protection Regulation (GDPR) seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and students are expected to save all data relating to their work to their laptop/tablet or the School's central server / Google Drive Account.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required to fulfil their role. No personal data of staff or students should be stored on personal memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager.

## **8.0 Password security**

Students and staff have individual school network logins, email addresses and storage folders on the server. Staff and students are regularly reminded of the need for password security. All students and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every three months;
- not write passwords down; and
- not share passwords with other students or staff.

## **9.0 Safe use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or

downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their images on the internet (e.g. on social networking sites).

Parents/carers are welcome to take videos and digital images of their children at school events for their personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites etc. without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other students in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims but must follow this policy and the Acceptable Use Policy and Early Years Mobile Phone and Camera Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Students must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before photographs of students are published on the school website, see Parent Contract for more information.

Photographs published on the school website, or displayed elsewhere, that include students, will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

## **10.0 Misuse**

The School will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and other relevant agencies or enforcing authorities. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek external assistance. This includes, but is not limited to, involvement in cyberbullying, 'sexting' or sharing youth-produced sexual images, involvement in radicalisation, grooming and other high-risk activities.

Incidents of misuse or suspected misuse must be dealt with by staff following the school's policies and procedures detailed in the Safeguarding and Child Protection Policy.

The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Anti-Bullying Policy.

## **11.0 Electronic Devices - search and deletion**

The School has the authority to search students for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

The Executive Principal may authorise any staff member to search students and to seize anything they have reasonable grounds for suspecting is a prohibited item or is evidence concerning an offence. If a member of staff finds a pornographic image, they should immediately bring this to the attention of the DSL or Executive Principal who may dispose of the image unless its possession constitutes a specified offence (i.e. it is extreme or child pornography) in which case it must be delivered to the police as soon as reasonably practicable.

Images found on a mobile phone or other electronic device can be deleted unless it is necessary to pass them to the police. Where the person searching finds an electronic device they may examine any data or files on the device if they think there is a good reason to do so. Following an examination, if the person 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.

The member of staff must have regard to the local regulations and guidelines when determining what is a "good reason" for examining or erasing the contents of an electronic device. In determining a 'good reason' to examine or erase the data or files, 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 the teacher must consult with the DSL or one of the Heads of School 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.

All school staff should be aware that behaviours linked to sexting put a child in danger. The School Board should ensure sexting and the School's approach to it are reflected in the Safeguarding and Child Protection policy.

## **12.0 Loading/installing software**

For this policy, software relates to all programmes, images or screensavers, which can be downloaded or installed from other media:

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free of viruses.
- Only authorised persons, such as the ICT Technician or Computing Subject Leader, may load software onto the school system or individual computers.
- Where staff are authorised to download software to their laptops/devices, they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

### **13.0 Backup and disaster recovery**

The School will define and implement a backup regime which will enable recovery of critical systems and data within a reasonable timeframe should a data loss occur. This regime should include:

- The use of a remote location for backup of crucial school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system.
- No data should be stored on the C drive of any curriculum computer as it is liable to be overwritten without notice during the process of ghosting the computers.
- Staff are responsible for backing up their data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server.
- Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.

The School should also define a whole school ICT disaster recovery plan which would take effect when a severe disturbance to the schools ICT infrastructure takes place, to enable critical school systems to be quickly reinstated and prioritised, including who would be involved in this process and how it would be accomplished.

### **14.0 Guidance on Bring Your Own Device (BYOD) Policy for Staff and Visitors**

The School recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective, and visitors. Our school embraces this technology but requires that it is used acceptably and responsibly.

This policy is intended to address the use by staff members and visitors to the school of non-school owned electronic devices to access the internet via the school's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school. These devices include smartphones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy, please check with the school's IT team. These devices are referred to as 'mobile devices' in this policy.

This policy is supported by the Acceptable Use Policy.

### **15.0 Policy statements**

#### 15.1 Use of mobile devices at the school (Visitors/Staff)

Staff and visitors to the School may use their own mobile devices in staff only areas or the Staff Room. Visitors may only use their phones around the site with the express permission of the chaperoning staff member.

Staff and visitors to the school are responsible for their mobile devices at all times. The school is not responsible for the loss or theft of or damage to the mobile device or storage media on the device (e.g. removable memory card) however caused. Reception must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off when in a prohibited area and at a prohibited time and must not be taken into controlled assessments and examinations unless exceptional circumstances apply.

The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises. Mobile devices may not be used in the Early Years areas.

### 15.2 Use of cameras and audio recording equipment (Visitors/Staff)

Parents and carers may take photographs, videos or audio recordings of their children at school events for their personal use.

To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them.

Parents or carers should avoid commenting on activities involving students other than their own in photographs, video, or audio.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school.

### 15...2 Access to the school's internet connection (Visitors/Staff)

The School provides a wireless network that staff and visitors to the school may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the School, and the School may withdraw access from anyone it considers is misusing the network.

An access key to join the visitor wifi may be obtained from the IT Manager.

The School cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.

The School is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's device while using the School's wireless network. This activity is taken at the owner's own risk and is discouraged by the School. The School will have no liability whatsoever for any loss of data or damage to the owner's device resulting from the use of the School's wireless network.

### 15.3 Access to school IT services (Staff only)

School staff are permitted to connect to or access the following school IT services from their mobile devices:

- the School email system;
- the School MIS, Google Drive

Staff may use the systems listed above to view school information via their mobile devices,

including information about students. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for staff to download school information to their mobile devices to view it (for example, to display an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it.

Staff must only use the IT services listed above and any information accessed through them for work purposes. School information obtained through these services is confidential, in particular information about students. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the school's IT team or Executive Principal as soon as possible. Staff must not send school information to their email accounts.

If in any doubt a device user should seek clarification and permission from the school's IT team before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

#### *15.4 Monitoring the use of mobile devices (Visitors/Staff)*

The School may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network or IT systems. By using a mobile device on the School's IT network, staff and visitors to the School agree to such detection and monitoring. The School's use of such technology is to ensure the security of its IT systems, tracking school information.

The information that the School may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content from school IT services or the school internet connection should report this to the School's IT team as soon as possible.

#### *15.5 Security of staff mobile devices (Staff only)*

Staff must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensure that the device auto-locks if inactive for a period.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff are reminded to familiarise themselves with the School's e-safety and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

### 15.6 Compliance, Sanctions and Disciplinary Matters for staff (Staff only)

Non-compliance with this policy exposes both staff and the School to risks. If a breach of this policy occurs, the School will respond immediately by issuing a verbal then written warning to the staff member. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and permission to use the device on school premises will be temporarily withdrawn. For persistent breach of this policy, the School will permanently revoke permission to use user-owned devices in school.

### 15.7 Incidents and Response (Staff only)

The school takes any security incident involving a staff member's or visitor's device very seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to Reception in the first instance. Data protection incidents should be reported immediately to the Executive Principal who is the school's data protection controller.

## **16.0 Acceptable Use Policy**

This policy applies to all members of the School community, including staff, students, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

### 16.1 Online Behaviour

As a member of the School community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, material that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, phone number or social media accounts to contact students or parents, and students and parents should not attempt to discover or reach the personal email addresses, phone numbers or social media accounts of staff.

### 16.2 Using the School's IT systems

Whenever you use the School's IT systems (including by connecting your device to the network) you should follow these principles:

- Only access school IT systems using your username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not try to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.

Remember that the School monitors use of the School's IT systems, and that the School can view content accessed or sent via its systems.

### *16.3 Compliance with related school policies*

You will ensure that you comply with the school's e-Safety Policy, Safeguarding and Child Protection Policies and Anti-Bullying Policy.

### *16.4 Breaches of this policy*

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. Also, a deliberate breach may result in the School restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online, you should report it to the School's DSL. Reports will be treated with confidence

## **17.0 Complaints relating to all aspects of E-Safety**

As with all issues of safety, if a member of staff, a student or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Please see the Complaints Policy for further information.

## **Appendix 1 - Student Acceptable Use Agreement**

### **For my safety:**

- I understand that the School will monitor my use of the ICT systems, e-mail and other digital communications.
- I will not tell anyone my username or password nor will I try to use any other person's username and password.
- I will be aware of 'stranger danger' when I am communicating online.
- I will not give out any personal information (e.g. home address and telephone number) about myself or anyone else when online.
- I will not arrange to meet people offline that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I will report any online behaviour of others which makes me feel uncomfortable, or is inappropriate.

### **Respecting everyone's rights to use technology as a resource:**

- I understand that the School ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the School ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube) unless I have the permission of a member of staff to do so.

### **Acting as I expect others to behave 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 without their permission.

### **Keeping secure and safe when using technology in school:**

- I will only use approved e-mail or message accounts on the school system.
- I will only use my handheld/external devices (e.g. mobile phones, USB devices, etc.) in school if I have permission and I understand that if I do use my own devices in school, I must follow the rules as if I was using school equipment.
- I 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 (e.g. VPN) 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.
- I will not open any attachments to emails unless given permission to do so and I know and trust the person/organisation that sent the email.
- I will ask for permission before sending an email to an external person/organisation
- I will not install or attempt to install programmes of any type on a machine or store programmes on a computer, nor will I try to alter computer settings.
- I will immediately tell a staff member if I receive an offensive email or message.

### **Using the internet for research or recreation:**

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I should ensure that I have permission to use the original work of others in my work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

**Taking responsibility 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 include my membership of the school community (e.g. cyberbullying, inappropriate use of images and/or personal information).
- I understand that if I break these rules, I will be subject to disciplinary action as outlined in the School's Behaviour Policy. This may also include loss of access to the School network/internet.

I have read and understood the above and agree to follow the rules outlined.

Name:	
Signature:	
Date:	

## Appendix 2 - Parent/Carer Acceptable Use Agreement

The School seeks to ensure that students have good access to ICT to enhance their learning and, in return, expects students to agree to be responsible users. A copy of the Student Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the School expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the School in this important aspect of the School's work.

=====

### Acceptance of Use Form

Parent/Carer's Name:	
Student's Name:	

As the parent/carers of the above student, I understand that my son/daughter will have access to the internet and ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the School will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the School cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the School will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt the safe use of the internet and digital technologies at home and will inform the School if I have concerns over my child's e-safety.

Signature:	
Date:	

## Appendix 3 - Staff Laptop/Devices Acceptable Use Agreement

### 1. Introduction

- This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the School.
- It should be read in conjunction with the School's e-Safety Policy
- All recipients and users of these devices should read and sign the agreement.

### 2. Security of equipment and data

- The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
- Staff should understand the limitations of the school's insurance cover.
- Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

### 3. Software

- Any additional software loaded onto the laptop should be in connection with the work of the School. No personal software should be loaded.
- Only software for which the School has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
- Users should not attempt to make changes to the software and settings that might adversely affect its use.

### 4. Faults

- In the event of a problem with the computer, the School's ICT Technician/Network Manager should be contacted.

### Declaration:

I have read and understood the above and also the School's e-Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	

## Appendix 4 - Staff Acceptable Use Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the School's e-Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Executive Principal.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security, and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that personal data, particularly that of students, is stored securely through encryption and password and is used appropriately, whether in school, taken off the School premises or accessed remotely following the school e-Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with students (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that student use of the internet is consistent with the School's e-Safety Policy.
- When working with students, I will carefully monitor and scrutinise what students are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding students' safety to the appropriate person, e.g. e-Safety Coordinator and SLT member.

The School may exercise its right to monitor the use of the School's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes the unauthorised use of the School's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:	
Signature:	
Date:	