Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. In addition, the school uses images to market the school and to celebrate students' achievements and increasing numbers of parents wish to record their child's success in sport, drama and music, and students must have access to the internet for academic and leisure purposes. It is therefore important to have a robust and effective policy in place at the School.

Some of the dangers students may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers

Cyber-bullying (move)

- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. Behaviour, Anti-bullying and Child Protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school has provided the necessary safeguards to help ensure that everything that could reasonably be expected of us to manage and reduce these risks is in place. This e-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Schedule for Development/Monitoring/Review

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity

Scope of this Policy

This policy applies to all members of the school community (including all staff, students, volunteers, parents and visitors) who have access to and are users of school ICT systems, both in and out of school. This policy includes the use of ICT, mobile phones and other electronic devices, CCTV and data protection.

The Education and Inspections Act 2006 empowers Directors, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-- bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

The American Academy Larnaca Council

- The American Academy Larnaca Council is responsible for the approval of the E-Safety Policy

Director and Leadership Team

- The Director and the Leadership Team are responsible for the implementation and monitoring of this E-Safety policy as well as supporting those in school who carry out the internal e-safety monitoring role
- The Director is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated
- The Leadership Team will receive regular monitoring reports from the E-Safety Coordinator
- The Director and another member of the Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

E-Safety Coordinator

- leads the e-safety committee
- liaises with the Child Protection Officer
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- organises training and advice for staff
- liaises with school ICT technical staff

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to the Leadership Team

Network Manager and Technical Staff

With the explosion in technology, the Academy recognises that blocking and barring sites is no longer adequate. The school needs to teach all students to understand why they need to behave responsibly if they are to protect themselves. The school's technical staff has 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 hardware system, data and for training the teaching and administrative staff in the use of ICT. They monitor the use of the internet and emails and will report inappropriate usage to the pastoral staff.

The Network Manager and ICT Coordinator are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack. All equipment should be protected both physically and by software measures
- that Staff have all signed the Employee Acceptable Use Policy (Appendix A) and that students and their parents have signed the Students Acceptable Use Policy (Appendix B)
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy, (Appendix C) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation
- that monitoring software is implemented and updated as agreed in this and other school policies

Academic and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e--safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Employee Acceptable Use Policy (Appendix A). Flouting this policy is regarded as a disciplinary offence
- they report any suspected misuse or problem to the E-Safety Coordinator for investigation
- digital communications with students should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons and elsewhere in the school
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and must make sure that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Officer

The Academy recognises that internet safety is a child protection and general safeguarding issue. The DSP has been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. He/she works closely with the local agencies in promoting a culture of responsible use of technology that is consistent with the ethos of the school. All of the staff with pastoral responsibilities receive training in e-safety issues. The school's comprehensive PSHE programme on e-safety is the CPO's responsibility. He/she will ensure that all year groups in the school are educated as to the risks and the reasons why they need to behave responsibly online. It is his responsibility to handle allegations of misuse of the internet and should be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- cyber-bullying

Students

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy (Appendix B), which they and their parents will be expected to sign before being given access to school systems.
- must act reasonably and consider others e.g. do not download large files during peak times as this will affect other users
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Guardians

The Academy seeks to work closely with parents and guardians in promoting a culture of e-safety. We will always contact parents if we have any concerns about their children, and hope that parents will feel able to share any concerns with us. The Academy 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 is willing to provide discussion evenings for parents if necessary, either through a visiting specialist or by the school staff, in order to advise about the potential hazards, and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

Policy Statements

Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT and PHSE lessons and is regularly revisited – this covers both the use of ICT and new technologies in school and outside school
- Key e-safety messages are reinforced as part of a planned programme of assemblies, mentor times and pastoral activities
- Students are taught to be critically aware of the materials and content they access on-line and are guided to validate the accuracy of information. They are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students need to understand the need for the student AUP and will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT systems ("Student Acceptable use Policy") should be read, acknowledged and signed by all students and their parents
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- Updates to the e-safety will be communicated to all staff and it is their responsibility to read and understand the current policy

Technical Infrastructure

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

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Any actual or potential e-safety incident should be reported to the Network Manager and E-Safety Coordinator
- Both physical and non-physical (software based) security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data

LAN

- All users will have clearly defined access rights to school ICT systems
- Staff will not install programmes on school workstations / portable devices
- All users in the Senior School will be provided with a username and password by the IT department who will keep an up to date record of users and their usernames. All users will be required to change their password at the start of every academic year. In the Junior School group or class log-ons and passwords will be used, but teachers need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by students in this way should always be supervised and members of staff should never use a class log on for their own network access
- The administrator passwords for the school ICT system, used by the Network Manager are kept safely in a locked safe in the Treasury
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system will be in accordance with the relevant AUP

- Departing staff, students and visitors will have their access terminated on the last day of their employment

Internet / Web Filtering

- Access to the internet via the school's network will be filtered according to the document "the School web filtering policy"
- The school maintains and supports the managed filtering service
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Director (or other nominated senior leader)
- Any filtering issues should be reported immediately to the Network Manager
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Director of ICT, referring to ST if necessary. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- Users will not be able to download executable files
- The school infrastructure and individual workstations are protected by up to date anti-virus software, and by regular security updates
- The school will maintain a record of all staff and students who are granted access to the school's electronic communications on the basis of educational need
- All web activity is recorded and logs are retained for 1 month
- Abuses are reported to pastoral staff

School WiFi

- There is open access to the school WiFi for personal use
- This goes through the Web Filter so the same rules apply as above.
- The school takes no responsibility for any devices connected to the WiFi network
- The School reserves the right to block any device

CCTV

The use of CCTV can be affected by a number of Acts including the Data Protection Act, the Human Rights Act and the Regulation of Investigatory Powers Act (RIPA). The School works to comply with these Acts.

Signage

- The purpose for which the system has been installed is stated on signage and is placed in prominent positions to inform the public that they are entering an area where their images are being recorded
- The equipment is sited in such a way that it only monitors those spaces that are intended to be covered by the equipment
- Operators (staff who operate and monitor CCTV) are aware of the purposes for which the scheme has been established
- Operators are aware that they are only able to use the equipment in order to achieve the purposes for which it has been installed

Use of CCTV

The Academy will:

- Consider if CCTV is the only viable option prior to installation
- Ensure that the Data Protection Notification (public register completed by data controllers detailing what processing of personal data is being carried out and sent to the Information Commissioner) covers the purposes for which the equipment is used; Review both the use of the CCTV system and the procedures to ensure compliance with the law
- Not keep film/images for longer than necessary
- Process images in a lawful manner

At the point of obtaining images the following will be provided:

- The name and address of the school
- The name and address of party acting on behalf of data controller, alerting public to who is processing the CCTV images
- The purpose for which the images are intended to be used; and

- Any information which is necessary, having regard to the specific circumstances in which the images are, or are to be, processed to enable processing in respect of the individual to be fair

- Establish and document the person(s) who are responsible for ensuring day-to-day compliance with the requirements of the Code of Practice
- Make certain there are procedures for dealing with police enquiries

The Academy will not:

- Film areas that could amount to an infringement of personal privacy
- Ignore subject access requests (an individual's written request to access information about themselves under the Data Protection Act). A person identifiable on CCTV images may be entitled to view the footage and may make a request to do so
- Use CCTV footage for any other purpose other than what it was originally used for, e.g. prevention and detection of a crime
- Use covert monitoring without seeking legal advice
- Use Intrusive Surveillance at all
- Use inadequate equipment. Blurred or indistinct images could constitute as inadequate data, whilst poorly maintained equipment may not provide legally sound evidence
- Disclose data to third parties, unless it is lawful to do so
- Systematically monitor people by use of CCTV

The school infrastructure and individual workstations are protected by an up to date anti-virus curriculum

- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum. In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

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 and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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 own images on the internet e.g. on social networking sites
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes and the digital/video images must be deleted if no longer required
- 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 without their permission
- Photographs published on the website, or 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
- Written permission from parents will be obtained before photographs of students are published on the school website (may be covered as part of the AUP signed by parents at the start of the year
- Student's work can only be published with the permission of the student and parents

The school provides a folder on a specific drive for storage of all photographs taken at school events. These photographs cannot be used without permission from the E Safety Coordinator or used for private purposes. Records are kept in the Marketing Department of all students whose photographs cannot be used.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

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

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following activities are not allowed for both staff and students:

- Use of mobile phones in lessons (except when directed by the teacher)
- Taking photos or videos on mobile phones or other camera devices (without prior permission)
- Storage of student mobile phone numbers on personal phones for longer than necessary.

When using communication technologies the school considers the following as good practice:

Email

- All students and staff will be provided with a school email address
- The official school email service may be regarded as safe and secure
- Users need to be aware that email communications may be monitored
- Users must immediately report, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students or parents must be professional in tone and content
- Students must be taught about email safety issues, such as the risks attached to the use of personal details. They must also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Staff should only use School email accounts to communicate with students and other staff and external organisations if it involves school business
- Email sent via the School's system should not be considered private and the School reserves the right to monitor email
- Students should be reminded NOT to reveal any personal details of themselves or others in ANY communication, email or otherwise

Social Networking / Social Media

- Refer specifically to the School Social Media Policies, for (a) Staff and (b) Students
- We recognise that social networking and e-safety go hand-in-hand, so in addition to those separate policies, consider the following guidelines and precautions:

- Students should be taught about the use of social networking sites and the risks associated with revealing information
- Students are advised through ICT lessons and PSHE never to give out personal details of any kind which may identify them and their location. Examples include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of family/friends, specific interests and clubs etc
- Students are advised not to place personal photographs on any social networking site. They are advised to consider how public the information is and consider using private areas
- The school maintains a very active social networking presence, using Facebook, Twitter, blogs, and more. These accounts are all centrally controlled by the marketing department with careful password protection
- Staff and students should be aware of the dangers of communicating via personal networking sites and should try to communicate through the official school social networking accounts
- If personal publishing is to be used with students then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be monitored by school staff. (What does this actually mean? What's the scenario here?)
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private
- Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control
- For responsible adults social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image once published
- All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status

School Website

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff
- The School's website must not contain any personal information of staff or students
- When information is placed on the School's website consideration must be given to intellectual property rights and copyright
- The content of the School's website should be reviewed regularly to ensure that all material is appropriate for the intended audience
- Publishing of any images of students can only take place with the permission of their parents and then must be decent and not reveal personal information

Mobile Phones

- Mobile phones, iPods, iPads and other personal electronic devices should be switched off and stored securely during the school day. They may be used in an emergency
- Staff may confiscate personal equipment that is being used during the school day for periods of up to 3 days
- Sanctions may be imposed on students who use their electronic equipment without consideration for others

Unsuitable/Inappropriate Activities

The Academy will not tolerate any illegal material, and will always report illegal activity to the police. If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the police. We 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.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Users shall not:

- use school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- reveal or publicise confidential or proprietary information (e.g. financial/ personal information, databases, computer / network access codes and passwords)
- create or propagate computer viruses or other harmful files
- carry out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Students

The following will be referred to the Police: Deliberately accessing or trying to access material that could be considered illegal including:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The following will be subject to disciplinary action:

- Unauthorised use of mobile phone / digital camera / other handheld device
- Unauthorised use of social networking / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another student's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Staff

The following will be referred to the Police:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)

The following will be subject to disciplinary action:

- Allowing others to access the school network by sharing username and passwords or attempting

to access or accessing the school network, using another person's account

- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations

If members of staff suspect that misuse might have taken place it is essential that this is reported appropriately and promptly.

Related Policies

- Student Acceptable Use Policy
- Staff Acceptable Use Policy
- Anti-Bullying Policy
- Behaviour Policy
- Social Media Policies for Staff and Students
- Data Protection Policy
- Safeguarding and Child Protection Policy

September 2022