e-Safety Policy

Incorporating:

Social Media
Use of Mobile Phones
Digital Photography
Use of School Resources outside School
Acceptable Use Agreement

Creation date	Autumn 2016
Adopted by Governors	Autumn 2016
Reviewed by	Assistant Headteacher – Student Learning and progress / SENCO
Review Date	Autumn 2023
Next Review Date	Autumn 2026

Headlands School – e-Safety Policy

Contents:

Introduction

We believe that ICT, social media and social networking plays a critical role in equipping students for life in the 21st Century, it can also have a positive impact on teaching and learning. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both inside and outside of the classroom. This policy has been drawn up to protect all parties – the students, the staff and the school, and aims to provide clear advice and guidance on how to minimise risks and deal with any infringements.

The rapid change of technology and the adoption of this into our lives is growing year on year. The e-Safety Policy recognises these changes and takes the viewpoint that if clear policies, strategies, training and procedures are in place and embedded, both in the curriculum and teaching practice the use of these technologies in school can bring benefits in terms of learning, development and engagement.

The e-Safety policy will focus on empowering the user to manage the risks faced by life in a digital world through effective, well established, up to date training and evaluation. This will develop a culture of awareness of digital safety both in and outside of the school environment for Students, Parents and Staff.

This Policy should be considered in conjunction with:

- Headlands School Safe Working Policy
- Headlands School Behaviour for Learning Policy
- ERSCB Staff & Volunteer Code of Conduct
- ERYC Harassment / Bullying Policy
- ERYC Data Protection Policy
- ERYC Internet Usage Policy
- ERYC Social Media Guidelines
- Persistent or Vexatious Complaints/Harassment Policy

Responsibilities of the School Community

We believe that e-Safety is the responsibility of the whole school community. Everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team

- Develop and promote an e-Safety culture within the school community.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to e-Safety effectively.
- Receive and regularly review e-Safety incident logs and be aware of the procedure to be followed should an e-Safety incident occur in school.
- Take ultimate responsibility for the e-Safety of the school community.
- The e-Safety Coordinator, Assistant Headteacher – Student Learning and Progress/SENCO has undertaken the CEOP Ambassadors training programme and regularly attends LA e-Safety updates.

Responsibilities of the e-Safety Coordinator (Assistant Headteacher)

- Regularly review and maintain the school's e-Safety Policy in association with ERYC policies and guidance regarding e-Safety, Internet Usage and Social Media.
- Promote an awareness and commitment to e-Safety throughout the school.
- Be the first point of contact in school on all e-Safety matters.
- Develop an understanding of current e-Safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive appropriate e-Safety training through regular updates.
- Ensure that e-Safety education is embedded into the curriculum.
- Ensure that e-Safety is promoted to Parents/carers through a regularly updated part of the school website, newsletters to parents and e-Safety surgeries held during Parents' Evenings.
- Liaise with the Local Authority, the local Safeguarding Children's Board and other relevant agencies as appropriate.
- Monitor and report on e-Safety issues to SLT and Governors as appropriate.
- Ensure an e-Safety incident log is kept up-to-date.
- Ensure that incidents of cyber-bullying, identified through cyber mentors Student Service Leaders, are dealt with effectively and are clearly identified on the schools Incident Log.
- Ensure the development, implementation and regular review of an action plan to ensure that a planned, comprehensive and age related e-Safety program is delivered across the school.

`

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's e-Safety Policy and associated ERYC policies and guidance regarding e-Safety, Internet Usage and Social Media.
- Develop and maintain an awareness of current e-Safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed e-Safety messages in learning activities where appropriate.
- Supervise students carefully when engaged in learning activities involving technology.
- Be aware of what to do if an e-Safety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Technical Staff

- Read, understand and help promote the school's e-Safety Policy and associated ERYC policies and guidance regarding e-Safety, Internet Usage and Social Media.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school ICT system.
- Report any e-Safety related issues that come to their attention to the e-Safety Coordinator.
- Develop and maintain an awareness of current e-Safety issues, legislation and guidance relevant to their work.
- Liaise with the Local Authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Students

- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for their own and each other's' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by students outside of school.
- Respect the feelings, rights, values and intellectual property of others in the use of technology in school and at home.
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if they know of someone who this is happening to.
- Discuss e-Safety issues with family and friends in an open and honest way.
- Report issues directly to any member of staff.

Responsibilities of Parents/carers

- Help and support the school in promoting e-Safety.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss e-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with the school if there are any concerns about their children's use of technology.

Responsibilities of the Governing Body

- Read, understand and help promote the school's e-Safety Policy and associated ERYC policies and guidance regarding e-Safety, Internet Usage and Social Media.
- Develop an overview of the benefits and risks of the Internet and common technologies used by students.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages students to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the e-Safety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging Parents/Carers to become engaged in e-Safety activities.
- Ensure appropriate funding and resources are available for the school to implement their e-Safety strategy.

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives, not just in school but outside as well, and we

believe we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings. To this end we will:

- Provide a series of specific e-Safety-related lessons in Years 7, 8 & 9 as part of the ICT curriculum.
- Provide specific e-Safety related sessions in Years 10, 11 and the Sixth Form.
- Discuss, remind or raise relevant e-Safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- Remind students about their responsibilities through an IUP which every student will accept when they login to their accounts.

How Parents/carers will be involved

We believe it is important to help all our Parents/carers develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Include useful links and advice on e-Safety regularly in newsletters and on our school website.
- Invite feedback on e-Safety from Parents/carers.

Managing ICT Systems and Access

- The school will be responsible for ensuring that access to ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to date.
- All staff will sign an Acceptable Use Agreement (Appendix A). Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- Students will access the Internet using an individual log-on, which they will keep secure. Whether supervised by a member of staff, or working independently, students will abide by the school e-Safety Policy at all times.
- Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow students to access the Internet through their log-on. They will abide by the school e-Safety Policy at all times.
- Administrator passwords and access details for the schools' ICT systems are known by the school's ICT Support team. Further details of this can be found in the school's disaster recovery / business continuity plan.
- The school prevents unauthorised and inadvertent access to the wireless network (where coverage is available) using Network Authentication and Proxy Server Authentication for access to the Internet.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish that the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate. The school will regularly review the Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet Access

- The school uses a BT Internet Feed with no access to sites that are on the IWF banned list. The school uses Lightspeed filtering configured to have different levels of filtering dependent on key stage / subject and age.
- The school uses a Sonicwall Firewall which helps secure the schools network from unauthorised access.

- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-Safety Coordinator (Assistant Headteacher – Learning and Progress/SENCO).
- If users discover a website with potentially illegal content, this should be reported immediately to the e-Safety coordinator. The school will report this to appropriate agencies including the, Local Authority, CEOP or IWF.
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning Technologies in School

	Students	**Staff**
Personal mobile phones brought into school.	Allowed	Allowed
Mobile phones used in lessons	Allowed only for curriculum purposes with permission from staff	Allowed only for curriculum purposes
Mobile phones used outside of lessons	Not allowed	Allowed
Taking photographs or videos on personal equipment	Allowed only for curriculum purposes **with permission from staff**	Allowed for curriculum purposes providing they do not include pictures of groups or individual students
Taking photographs or videos on school devices	Allowed for curriculum purposes	Allowed for curriculum purposes
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Allowed only for curriculum purposes **with permission from staff**	Allowed for curriculum purposes
Use of email to contact Staff or Student	Allowed for curriculum purposes using the school student and staff emails	Allowed for curriculum purposes using the school student and staff emails
Use of personal e-mail addresses in school	Not allowed	Allowed at certain times
Use of school e-mail address for personal correspondence	Not allowed	Allowed
Use of online chat Rooms	Allowed via Moodle All other instances not allowed	Staff allowed via Moodle. All other instances not allowed
Use of instant messaging services.	Not allowed	Not allowed
Use of blogs, wikis, podcasts or social networking sites	Allowed via Moodle All other instances not allowed	Allowed via Moodle All other instances not allowed
Use of video conferencing or other online video meetings	Allowed with supervision by staff	Allowed

Using Email

- Staff and students should use approved email accounts allocated to them by the school, and be aware that their use of the school email system will be monitored and checked.
- Communication between staff and students or members of the wider school community should be professional and related to school matters only.
- Students will be allocated an individual email account for their use in school.

- Students must be reminded that, when using email, they should send polite and responsible messages. Also, about the dangers of revealing personal information, opening an e-mail from an unknown sender, or viewing/opening attachments.
- Students are not permitted to access personal email accounts during school.
- Any inappropriate use of the school email system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.
- Headlands School email should not be used to send inappropriate messages or information pertaining to staff or students.

Using Images, Video and Sound

- Students should be reminded of safe and responsible behaviours when creating, using and storing digital images, video and sound. Also, of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Staff and students will follow this policy when creating, using and storing digital resources.
- In particular:
    - digital images, video and sound will not be taken without the permission of participants;
    - images and video will be of appropriate activities and participants will be in appropriate dress;
    - full names of participants will not be used within the resource itself, within the file-name or in accompanying text online;
    - such resources will not be published online without the permission of the staff / students involved.
- If students are involved, relevant parental permission will also be sought before resources are published online.

Using Video Conferencing and other online video meetings

Video conferencing may be used to enhance the curriculum by providing learning and teaching activities that allow students to link up with people in other locations and see/hear each other. However, staff and students must take part in these opportunities in a safe and responsible manner.

- A member of staff must supervise all video conferencing activity.
- Students must not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
- Video conferencing equipment will be switched off and secured when not in use.
- Students will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Video conferencing should not take place off school premises without the permission of the Headteacher.
- Parental permission will be sought before taking part in video conferences.
- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

Using New Technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-Safety point of view.

We will regularly amend the e-Safety Policy to reflect any new technology that we use, or to reflect the use of new technology by students which may cause an e-Safety risk.

Protecting Personal Data

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018 and ERYC Data Protection Policy.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the Headteacher, and without ensuring such data is kept secure.

- Data which is personal or sensitive must not be projected onto any whole class display e.g. interactive whiteboard.

The School Website and other online content published by the school

- The school website will not include the personal details, including individual e-mail addresses of staff or students. A generic contact e-mail address will be used for all enquiries received through the school website.
- All content included on the school website will be approved by the Headteacher before publication.
- The content of the website will be composed in such a way that individual students cannot be clearly identified.
- Staff and students must not post school-related content on any external website without seeking permission first.

Using Blogs, Wikis, Podcasts, Social Networking etc. for students to publish content online

We may use blogs/wikis/podcasts to publish content online to enhance the curriculum by providing learning and teaching activities that allow students to publish their own content.

- Blogging, podcasting and other publishing of online content by staff and students should be pre-approved by the Headteacher before it is posted online.
- Students must seek approval from staff prior to posting online.
- Students will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, students will be reminded not to reveal personal information which may allow someone to identify and locate them. Students will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.
- Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.
- If social media sites are used, then staff should carry out a risk assessment to determine which tools are appropriate.
- The school's Acceptable Use Agreement makes it clear to students and staff what is allowed.

Use of social networking (social media) by staff in a personal capacity

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to **protect their professional reputation** by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

i. Staff must never add students as friends into their personal accounts.
ii. Staff must not post pictures of school events without the Headteacher's consent.
iii. Staff must not use social networking sites within lesson time.
iv. Staff need to use social networking in a way that does not conflict with the current National Teacher's Standards.
v. Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
vi. Staff must not post negative comments about the school, students, parents or colleagues including governors.
vii. Staff should read and comply with ERSCB 'School Staff & Volunteer Code of Conduct'.

Inappropriate use by staff should be referred to the Headteacher in the first instance or LADO (Local Authority Designated Officer).

Posts made by Parents/Carers

Parents and Carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion.

i. Parents are not expected to post pictures of students other than their own children on social networking sites.
ii. Parents should make complaints through official school channels and not by posting them on social networking sites.
iii. Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.
iv. Parents should be aware of the Persistent or Vexatious Complaints Policy, which aims to uphold standards of courtesy in respect of staff, students and the school community as a whole.

Dealing with incidents of online bullying.
The schools e-Safety Policy and/or Bullying/Harassment Policy makes sanctions regarding bullying using new technologies very clear.

DfE Guidance, 'Behaviour and Discipline in Schools', indicates that the school can take action against incidents that happen outside school if it:

i. Could have repercussions for the orderly running of the school or
ii. Poses a threat to another student or member of the public or
iii. Could adversely affect the reputation of the school.

Use of social networking sites to harass, bully or intimidate would be covered by this irrespective of when/where the post was made.

<u>Use of Mobile Phones and Digital Photography</u>

Children have their photographs taken in Years 7, 9 and 11 and are saved onto the schools Management Information System for identification purposes. **Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of school children during the school day, either for school or personal use.**

Procedures
a. Under the Data Protection Act 2018 the school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the schools Management Information System which is password protected. All photographs will be deleted from the school network 7 years after the student has left school.
b. The school's digital cameras must not leave the school setting (unless on an educational visit). Photographs are printed in the setting by staff and images are then removed from the camera memory.
c. Photographs may be taken during indoor and outdoor activities in school, but must be stored on the Staff Drive.
d. Often photographs may contain other students in the background.
e. Events such as Sports Day, Outings, Christmas and Fundraising events may be recorded by video and photographs by staff and parents/carers but always in full view of all attending. Parents must not post photographs or video containing other students on social media websites (See above, Posts by Parents/Carers).
f. On occasion the school might like to use photographs of students taking part in an activity to advertise/promote the school via the website etc., however in this instance; specific parental permission must be obtained with approval from the Headteacher.
g. Many mobile phones have built in cameras so staff mobile phones must not be used to take pictures of students in our school. **Visitors may only use their personal mobile phones in the foyer or outside the building and should be challenged if seen using a camera inappropriately or photographing students.**
h. The use of cameras and mobile phones are prohibited in toilets.
i. Staff are asked not to make personal calls during their working hours. However, in urgent cases a call may be made or accepted if deemed necessary and by arrangement with the Headteacher.
j. All school cameras and videos should be kept securely locked away at all times and used with appropriate authority.

Acceptable Use

Headlands School aims to ensure that staff and volunteers have good access to digital technology to enhance their work and the learning opportunities for students. In return, Headlands School expects staff and volunteers to adhere to the Acceptable Use Agreement (Appendix A) and confirm they will be responsible users.

- Staff and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- Headlands School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of technology in their everyday work.

Use of School Resources (outside school)

Members of staff, may from time to time, wish to borrow items of school equipment for use at home. Staff are permitted to do this as long as the loan is cleared with and noted by the Director of Curriculum Area or member of SLT and a dated & signed entry marked in a departmental log. The responsibility for loss, damage or theft lies with the member of staff concerned and they should be satisfied that they have adequate insurance in place should any accident/theft occur whilst the item is in their care.

Staff who have laptops allocated to them to carry out their role should ensure that these are covered under appropriate personal insurance e.g. contents insurance, and these must be returned to the school if they are no longer required or the individual ceases employment at the School.

You should be aware that staff will be responsible for the replacement of any equipment damaged, lost or stolen whilst away from the school premises.

It is the responsibility of the Directors of Curriculum Area/relevant school manager to inform the school office if any inventory items allocated to their department are damaged, lost or stolen so that this can be recorded and authorised by the Headteacher in the inventory log books.

Non-moveable resources may be used, again with the due permission of a Director of Curriculum Area or member of SLT. If equipment is being used on school premises during holiday periods then not only must prior clearance with Compass be obtained but the Safety, Health & Environment Manager should also be notified for access arrangements.

Any damage should be immediately reported.

The e-Safety Policy will be reviewed regularly and updated in line with current requirements.

Appendix A

Acceptable Use Agreement

The Headlands School Acceptable Use Agreement recognises the increasing importance of the use of new and evolving technologies within the lives of all and in particular within the business and administration uses of Headlands School. In today's environment access and use of efficient systems is a must. All users should therefore have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Agreement 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 Headlands School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

Headlands School will try to ensure that staff and volunteers will have good access to digital technology 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.

Acceptable Use Agreement

I understand that I must use the school's technology in a responsible way, to ensure that there is no risk to my safety or to the safety of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that Headlands School will monitor my use of digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, mobile phones, email, VLE etc.) in any environment on or off Headlands School site. This also applies to the use of any personal data (digital or paper based) to which I have access.
- I understand that ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by Headlands School.
- I will not disclose any passwords to anyone else, nor will I try to use any other person's passwords. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using the school's technology:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the relevant policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the School website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in accordance with the relevant policies.
- I will only communicate with students and parents / carers using official IT systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

Headlands School have the responsibility to provide safe and secure access to technologies to ensure the smooth running of the schools' IT systems:

- When I use my personal mobile devices (laptop / tablets / mobile phones / USB devices etc.) anywhere, I will follow the rules set out in this agreement, in the same way as if I was using schools owned equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date encryption software, anti-virus software and are free from viruses. Non-encrypted devices are not permitted.
- Removable devices such as USB external hard drives and USB memory sticks must be encrypted before used to store Headlands School data. Please speak to ICT support who will be able to encrypt your device for you. Non-encrypted drives are not permitted.
- School owned mobile phones must be secured by a pin code / password or fingerprint if possible.
- All devices used to access / store school data must be entered onto an Inventory, this will be managed by ICT Support and used for audit purposes only. Devices not logged with ICT Support must not be used to hold / access school data.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my work is regularly backed up, in accordance with relevant School policies. This includes data stored on personal / school owned removable drives.
- I will not try to upload, download or access any material which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users being able to carry out their work.
- 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, unless this is authorised by ICT Support.
- I will not disable or cause any damage to School equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable secure storage. All losses of such data must be reported immediately.
- I understand that the Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by a School policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- The loss or theft of removal storage devices and laptops must be reported to ICT Support immediately.

When using the internet in my professional capacity or for School sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- When I access the internet for personal use this will not compromise my duties and will not be during agreed working hours.

I understand that I am responsible for my actions in and out of my normal place of work:

- I understand that this Acceptable Use Agreement applies not only to my work and use of School digital technology equipment, but also to my use of IT systems and equipment off site and the use of any personal equipment for School purposes.

- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action or any other action pertinent to my role. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.