e-Safety Policy

Reviewed by	Ross Bonnett
Last Reviewed date	Summer 2017
Next Review Date	Summer 2019

Headlands School

e-Safety Policy

Contents:

Introduction

We believe that ICT has a critical role in equipping students for life in the 21st Century and that ICT can 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 in and outside of the classroom. This policy document 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 how to 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:

- The Anti-bullying Harassment and Discrimination Policy.
- The Behaviour for Learning Policy
- The Child Protection Policy
- The Data Protection Policy
- The Internet Usage Policy (IUP)

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 for Personal Development, Behaviour and Welfare has undertaken the CEOP Ambassadors training programme and regularly attends LA e-safety updates.

Responsibilities of the e-safety Coordinator (Assistant Headteacher)

- Promote an awareness and commitment to e-safety throughout the school.
- Be the first point of contact in school on all e-safety matters.
- Lead the school e-safety group, which meets at least every half term. See appendix A.
- Create and maintain e-safety policies and procedures.
- 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 from the e-safety Coordinator.
- 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 the e-safety group, SLT and Governors as appropriate.
- Ensure an e-safety incident log is kept up-to-date.
- Ensure that incidents of cyber-bullying, identified through the cyber mentors or otherwise are dealt with effectively and are clearly identified on the schools bullying 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.
- Ensure HELP, the school's on-line reporting system, is monitored daily and that referrals made are passed to the appropriate persons and support/intervention is arranged.

`

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's e-safety policies and guidance.
- Read, understand and adhere to the school Internet Usage Policy (IUP) – Staff and Students.
- 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, contribute to and help promote the school's e-safety policies and guidance.

- Read, understand and adhere to the school staff IUP.
- 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

- Read, understand and adhere to the school IUP - Students.
- Help and support the school in creating e-safety policies and practices; and adhere to any policies and practices the school creates.
- 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 either directly to staff or using HELP the schools on-line reporting system.

Responsibilities of Parents / Carers

- Help and support the school in promoting e-safety.
- Read, understand and promote the school IUP with their children.
- 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, contribute to and help promote the school's e-safety policies and guidance.
- 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.

Learning and Teaching

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 the 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 users will sign an Internet Usage Policy (IUP) provided by the school, appropriate to their age and access. 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 IUP 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 IUP 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 if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. We will regularly review our 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 for Personal Development, Behaviour and Welfare).
- 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, LA, 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 form staff.	Allowed only for curriculum purposes.
Mobile phones used outside of lessons.	Students allowed, during break, lunch times and pre and post school.	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 e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.
- Students will be allocated an individual e-mail account for their use in school.
- Students will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Students are not permitted to access personal e-mail accounts during school.
- Communication between staff and students or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.
- Email should not be used to send any personal or sensitive information pertaining to students.

Using Images, Video and Sound

- We will remind students of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them 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 the school policy on 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 either 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 Blogs, Wikis, Podcasts, Social Networking and other ways 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 pupils should be pre-approved by a member of staff before it is posted online.
- Any blogs run by school staff on behalf of the school **must** be pre-approved by the member of staff before publishing.
- 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.

Using Video Conferencing and other online video meetings

- We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow students to link up with people in other locations and see and hear each other. However, we will ensure that staff and students take part in these opportunities in a safe and responsible manner:
- A suitable member of staff will supervise all video conferencing activity.
- Students will 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 1998.
- 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 sent via email.
- 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 should not post school-related content on any external website without seeking permission first.

This Policy will be reviewed regularly and updated in line with current requirements.

Appendix A.

The Headlands School e-safety Group

Mandate
To ensure that:

- All members of the school community (including students, all staff, governors and parents) are educated in regard to the safe use of technology, and that this education remains current and reflects the ever changing nature of technology.
- Appropriate mechanisms to intervene and support staff, students and parents when an e-safety incident has occurred, are available.
- This training/intervention and support takes into account the 3 main areas of risk:
    - **Content –** being exposed to illegal, inappropriate or harmful material
    - **Contact –** being exposed to harmful online interaction with other users
    - **Conduct -** personal online behaviour that increases the likelihood of, or causes, harm.

This will be achieved by:

- Monitoring the ever-changing nature of e-safety requirements in the Headlands School Community.
- Regularly auditing the training needs of all members of Headlands School to ensure training is matched to need.
- Ensuring that a comprehensive, planned, age related e-safety curriculum is in place for all students and that this remains current.
- Promoting an understanding that technology is, and will continue to, evolve and change rapidly, and that our understanding of e-safety and subsequent education/training must also evolve to keep pace with this.
- Ensuring that all staff have a shared responsibility for ensuring e-safety.
- Creating a climate where new technologies can be harnessed to enhance learning through “managed” rather than “locked down” systems.
- Coordinating the delivery of specific events
- Maintaining and analysing the e-safety incident log and arranging appropriate intervention and support.
- Monitoring HELP, the school’s on-line reporting system, and arranging appropriate intervention and support.