Ludlow Church of England School

E-Safety Policy

Approved and signed: _____

On behalf of the Strategy and Resources Committee

Approved: 18th May 2015

Review Date: July 2018

Writing and reviewing the e-safety policy

The E-Safety Policy relates to other policies including, Child Protection and Anti-Bullying.

- The school's e-safety co-ordinator, is also the Child Protection Designated Lead, as the roles overlap.
- Our E-Safety Policy has been written by the school, building on best practice and government guidance.
- It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed annually.
- It was approved by the Governors on: 18th May 2015

Teaching and Learning

Why internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- The school internet access is provided by Shropshire Council through a regional broadband contract, which includes filtering appropriate to the age of students.
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Students will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be shown how to publish and present information appropriately to a wider audience.

Students will be taught how to evaluate internet content

- The school will seek to ensure that the use of internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will be taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon.
- For students whose parents lack economic or cultural educational resources, the school should build digital skills and resilience, acknowledging the lack of experience and internet at home.
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

Managing internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Education Technology Service (ETS) and The Bishop Anthony Educational Trust (BAET).

E-mail

- Students and staff may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to student email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the website should be the school address, email and telephone number. Staff or students' personal information will not be published.
- The headteacher, or nominee, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully. The school will use photographs only when permission has been granted by the parent/carer.
- Students' full names will be avoided on the website or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained as part of the admission process, before photographs of students are published on the school website.

Social networking and personal publishing on the school learning platform

- The school has a robust social media policy.
- The school will access social media sites if concerns are raised, and educate students in their safe use e.g. use of passwords.
- Students will be advised never to give out personal details of any kind which may identify them or their location, or place personal photos on any social network space provided in the school learning platform.
- Students and parents will be advised that the use of social network spaces outside school brings a range of opportunities; however, it does present dangers for primary and secondary aged students.

Managing filtering

- The school will work in partnership with ETS and BAET to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, the site must be reported to the E-Safety Coordinator and/or the ICT Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A log of any incidents may be useful to identify patterns and behaviours of the students.

Managing videoconferencing (if available)

- Videoconferencing will use the educational broadband network to ensure quality of service and security.
- All videoconferencing will be managed and supervised by the teacher.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity.
- The sending of abusive or inappropriate text messages is forbidden.
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with students is required.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulations 2018.

Policy Decisions

Authorising internet access

- All staff, governors and visitors must read and sign the "Acceptable Internet and Computer Use Policy for Staff, Governors and Visitors" before using any school ICT resource. (Appendix 1)
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- Parents will be asked to sign to acknowledge they have read and agreed to the "Acceptable Internet and Computer Use Policy for Students" (Appendix 2)
- Students must agree to comply to the "Acceptable Use of the Internet Statement" when applying for internet access. (Appendix 3)

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BAET can accept liability for the material accessed, or any consequences of internet access.
- The school will monitor ICT use to establish if the e-safety policy is adequate and that the implementation of the E-Safety Policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse will be overseen by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a Child Protection nature must be dealt with in accordance with the school's Child Protection procedures.
- Students and parents will be informed of the complaints procedure.
- Students and parents will be informed of consequences and sanctions for students misusing the internet, and this will be in line with the school's Behaviour Policy.

Introducing the E-Safety Policy to students

- Appropriate elements of the E-Safety policy will be shared with students as part of the induction process in year 7, and further curriculum opportunities will be provided for students to gain awareness of e-safety issues and how best to deal with them. This will be addressed each year as students become more mature and the nature of newer risks can be identified.
- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and internet use, will be monitored.

Staff and the E-Safety Policy

- All staff will be advised of the school's E-Safety Policy and its importance explained.
- All staff will sign to acknowledge that they have read and understood the E-Safety Policy and agree to work within the agreed guidelines.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be advised on the use of social media, both at work and in their personal situation.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school's E-Safety Policy in newsletters and on the school website and updates will be given.
- The school will ask all new parents to sign the parent /student agreement when their child begins school.
- Parents are offered e-safety training annually, with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

Appendices:

1. "Acceptable Internet and Computer Use Policy for Students" – parent/carer guidance
2. "Acceptable Use of the Internet Statement" – student version

ACCEPTABLE INTERNET & COMPUTER USE STATEMENT FOR ALL STUDENTS

The computer system is owned by the school and/or the BAET and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Neither the school nor the BAET will be liable under any circumstances for any injury, distress, loss or damage to the student or the parents, which may arise directly or indirectly from the student's use of the Internet facilities, the use of e-mail, or from other students' unauthorised use of those facilities or e-mail.

- Permission will be sought from students and parents before any personal data, i.e. names and photographs, are published on a web site;
- Access must only be made via the authorised account and password, which must not be made available to any other person;
- All Internet use should be appropriate to staff professional activity or student's education;
- The downloading of sexist, racist, pornographic, indecent or abusive images, text or sound files is forbidden;
- The downloading of any program, screen saver, game etc without permission from an authorised person is forbidden;
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden;
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received;
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded;
- The sending of 'sensitive personal data' whether relating to the sender or not is forbidden unless it is processed for reasons outlined in the school Data Protection Policy and the GDPR regulations 2018.
- The sending of any information which students are not certain to be 'public knowledge' outside the school is forbidden;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Copyright of materials and intellectual property rights must be respected;
- Legitimate private interests may be followed, providing school use is not compromised;
- No unauthorised contract, purchase or payment should be made over the Internet;
- Student purchases over the Internet are forbidden;

- Students are forbidden to access social networking sites such as Facebook;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Staff and students should be aware that Internet access is monitored and reported to the Headteacher.

ACCEPTABLE USE OF THE INTERNET

Student's Agreement

You must have the written permission of a parent or guardian before you can use the internet in school.

You are only able to use it to access materials for use in lessons and to help with your learning. The school will keep a record of the times you use the internet and all the sites you have visited.

I agree to the following:

- I will only use the internet for school work and will not visit chat rooms or any other unsuitable sites
- I will not access any areas of the internet that are inappropriate or offensive
- If any unsuitable material appears when I am using the internet I will report it to a teacher
- I accept responsibility to keep copyrighted material from being downloaded into the school
- I will not give personal information including credit card numbers, postal or email addresses, telephone or fax numbers, or use photographs of any other students, any adult or myself.
- I will always respect the privacy of files of other users. I will not enter the file areas of any other person
- I will not disclose any password or login name to anyone, other than the person responsible for running and maintaining the system
- I will be polite and use appropriate language in all my ICT communications
- I agree to staff having the right to view any material I use in the school's computers
- If I use material or CD ROMs in my work, I will always list this in a bibliography. I will select the information I need and present it in my own words
- I will not damage computers, computer systems or networks
- If I break any of the terms of this agreement, I know that one or more of the following will result:
- A ban, temporary or permanent on the use of the internet facilities at school
- A letter informing my parents of the rules I have broken
- Appropriate sanctions and restrictions placed on access to other school facilities
- Any other action decided by the Headteacher and Governors of the school