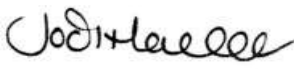
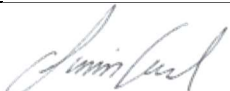




Our vision is to create an inclusive, friendly, safe and engaging learning environment which is grounded in our Christian values, enabling children to navigate obstacles, fulfil their potential and extend their horizons.

We value all members of our school community and encourage their individual talents and personalities so that each can shine in their own way.

Policy Name	E-Safety (Internet & Online) Policy
Date written:	August 2022
Date of last update:	11th July 2024
Date agreed and ratified by Governing Body:	18 th September 2018
Date of next full review:	September 2019
Signed by head Teacher: (Jodi Hacker)	
Signed by Chair of Governors: (Simon Curd)	

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Safeguarding.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.
- National Education Network standards and specifications.

School E-Safety Policy

The school has two members of staff that are conferenced with the e-safety policy; computing coordinator and the designated safeguarding lead.

This policy has been agreed by the senior management team and approved by governors.

Why Is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How Does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and access to learning wherever and whenever convenient.

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will regularly learn about E-Safety across the computing curriculum. They will learn how to make best and safest use of modern technology.
- Children have supervised access to learning enhancements sites such as Abacus and Purple Mash and Edshed; All of which can be accessed from home using passwords.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

E-MAIL

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- The school will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location

- Pupils will be advised not to place personal photos on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.

How Photography will be Managed

- The use of personal cameras is discouraged. Any photographs taken of children, must be made with the use of school cameras or other school technologies such as iPads and Tablets.
- The use of mobile phones for photography purposes is prohibited.
- Photographers should always ask for permission to take a photograph to ensure compliance of the data protection act. They should also get consent from parent, carer or guardian; see www.ico.gov.uk. In each case the consent of senior managers should be given before taking images or videos of children and young people. Parents are permitted to photograph (or video) their children, which may include incidental images of other children, on the understanding that such images or video should not be published in any form, particularly on social networking sites or other public forums. The school maintains a list of children (refer school office), who specifically must not be photographed or recorded under any circumstances.
- Care will be taken that photographs are stored appropriately.

Filtering

The school will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.

Update : July 2024 : As of April 2024 the Local Authority discontinued its Internet Provision to schools and after tendering for a new supplier, the school now maintains its own Firewall and Filtering Solution in conjunction with its preferred ISP. Both solutions meet or exceed the requirements for school Internet connectivity and filtering and are industry market leaders.

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.
- Staff should not use mobile phones to take pictures or videos of children. Staff should only use digital cameras which have been provided by the school. Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.

- Children who bring mobile phones to school are required to hand them in to the school office staff every morning and devices are collected at home time.

The Prevent Duty and E-Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the wellbeing of any pupil is being compromised.

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupil's Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

INFORMATION SYSTEM SECURITY

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

How Cyber Bullying Will be Managed

- Cyber bullying will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by cyber bullying.
- Concerned staff are expected to inform Mrs Hatcher, or Miss Rock.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Neither the school nor KCC can accept liability for the material accessed, or any consequences thereof.

These are other ways to minimise the risks to children-

- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990;
- Methods to identify, assess and minimise risks will be reviewed;
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken;
- The Headteacher will ensure that the policy is implemented effectively.

How Hawkhurst Primary School Will Ensure that Internet Access is Safe

Hawkhurst Primary School's chosen Internet Service Provider will operate a filtering system, which restricts access to inappropriate material. The methods they use fall in several overlapping types –

- **Blocking strategies** remove access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day.
- **A walled-garden or pass list** provides access only to a list of approved sites. Inevitably this approach will restrict pupils' access to valid information.
- **Filtering** examines the content of Web pages or e-mail messages for unsuitable words. Filtering of Web searches attempts to block a current loophole.
- **Filtering** searches using a range of safe search engines that are displayed in the computer suite :- <http://www.safesearchkids.com/google/>

None of these systems can be completely effective and a combination of approaches will be required, alongside adequate supervision. Should pupils access a site that is unsuitable they must tell their teacher who can then take appropriate action during the lesson (the teacher needs to get the site's

address). Afterwards they must inform the computing Co-ordinator who will then contact the schools chosen ISP to block the site.

Should an incident occur, it will be recorded on the e-safety incident proforma which can be found by asking the Computing Coordinator.

Handling E-Safety Complaints

All users of the school system must adhere to the rules of the school's e-safety policy. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance it is possible that the issue has arisen through Internet use outside school. Transgressions of the rules could include minor as well as the potentially serious incidents and a range of sanctions will be required.

- If an inappropriate site is accessed by a pupil by accident, this will be dealt with by the class teacher.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure. Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff will be trained in Safeguarding procedures, including elements of E-Safety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site. The school will also organise E-Safety workshops to support parents' understanding of how to best safeguard their children against potential online dangers.