Scarning VC Primary School

E-Safety and Acceptable Use Policy 20234
Adopted by FGB: 8.10.24

Review Date: September 2026

Writing and reviewing the E-safety policy

- The school will identify a member of staff who has an overview of E-safety, this would usually be the Senior Designated Professional (SDP).
  Stuart Howell (deputy head and DSL)

- 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.

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 curriculum and a necessary tool for staff and pupils.

- The school Internet access is provided by Norfolk County Council 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.

- Pupils will be educated in the effective use of the Internet

- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils 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 pupils complies with copyright law.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

- Pupils will be taught how to report unpleasant Internet content

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 Local Authority

E-mail

- **Pupils and staff 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.
- Staff to pupil 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 pupils 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 Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

- Nick King (head teacher) will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing photographs, images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.

- Pupils' names will be avoided on the Web site 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 before photographs or images of pupils are published

- Written permission from adults will be obtained before their names, photographs or images of themselves are published

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.

- Newsgroups will be blocked unless a specific use is approved.

- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

- Pupils must not place personal photos on any social network space provided in the school learning platform without permission.

- Pupils, parents and staff will be advised on the safe use of social network spaces

- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff.

- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- The school will use Norfolk County Council's web filtering service Netsweeper to ensure access to unauthorised websites are restricted.

- Netsweeper will send a daily monitoring report to the school's designated safeguarding leads which will indicate where a block has been initiated on pupil and staff devices, as a result of inappropriate content or security risks being identified.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing will be appropriately supervised for the pupils' age.

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.

Other devices

- The sending of abusive, offensive or inappropriate material is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.
- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read the 'Acceptable Use Policy' (see end of this policy) before using any school ICT resource.
- The school be responsible for ensuring that all staff and pupils who are granted access to school ICT systems are authorised to do so.
- Parents will be asked to sign and return a consent form.

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 Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.

Handling E-safety complaints

- 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 referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

- All staff will be given the School E-safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who 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 E-safety Policy in newsletters, the school brochure and on the school web site.

- Parents and carers will from time to time be provided with additional information on E-safety.

The school will ask all new parents to sign the parent /pupil agreement when they register their child

Scarning VC School Staff/Volunteers Acceptable Use Policy

To ensure that members of staff/volunteers/students are fully aware of their professional responsibilities when using information and communication systems equipment, all staff are asked to sign this Staff Acceptable Use policy.

I understand that the school ICT equipment and systems are the property of the school whether used on or off the premises.

ICT in school is defined as and not limited to: mobile phones, PDAs, digital cameras, laptops, desktop computers, netbooks ,ipads, visualisers, projectors, IWBs, photocopiers and printers.

I understand that my use of ICT in school, including Internet and email, is monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose or share any password or security information to anyone other than an authorised system manager.

I will not install any software or hardware without permission.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. I will take into account parental consent forms when taking photos and video.

I will respect copyright and intellectual property rights.

I will implement the school Response to an Incident of Concern procedure to deal with any incidents of concern.

I will ensure that all electronic communications that I make, including social networking, are compatible with my professional role.

I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will:
    - View and check any resources, including videos, before sharing them with or making them available to the children;
    - Ensure that search terms have been tested prior to sharing them with children and anything out of those terms is done discretely with the projector either frozen or turned off;
    - Ensure that children are made aware of e-Safety issues surrounding use of the Internet, including the age limits and legal restrictions on the use of social networking;
    - Ensure that any films or film clips, which are shown to the children, are registered as U or Uc. PG is not acceptable without explicit parental permission for that film.

Use of personal devices

- Use of personal smart phones and tablets is restricted to those times when children are not present
- No photos and videos are to be taken of children with such devices. Photos and videos of children should only be taken with school equipment
- When children are not around (e.g. after school) personal devices can be used to take pictures (e.g. displays)
- On external visit use of personal phone is permitted for communication (e.g. emergency, ETA). School equipment must be used for photos and videos.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.