Ernesford Grange Primary School

Online Safety Policy 2021

Date to be reviewed: September 2023

Headteacher: Ian Taylor

Date: September 2021

Online Safety

Online Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. This will include current new technology and how we should behave when using it.

The previous Internet E-Safety Policy has been extensively revised then renamed as Ernesford Grange's Online Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole including.

Ernesford Grange's Online policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum and Data Protection.

Teaching and Learning

Why is Internet use important?

Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. Ernesford Grange has a duty to provide students with quality Internet access as part of their learning experience.

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

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 functions.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- 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 networks of schools, support services and professional associations;

• improved access to technical support including remote management of networks and automatic system updates;

• access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Ernesford Grange's Internet access will be designed to enhance and extend education.

• Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

• The schools will ensure that the copying and subsequent use of internet-derived materials by staff and pupils complies with copyright law.

• Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

• Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.

• Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

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

• Pupils will use age-appropriate tools to research Internet content.

• The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

• Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.

• Users must take responsibility for their network use.

• Workstations should be secured against user mistakes and deliberate actions. • Servers must be located securely and physical access restricted.

• The server operating system must be secured and kept up to date.

• Virus protection for the whole network must be installed and current.

• Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

• The security of the school information systems and users will be reviewed regularly.

• Files held on the school's network will be regularly checked.

• The ICT coordinator/network manager will review system capacity regularly.

• The use of user logins and passwords to access the school network will be enforced.

How will email be managed when in use?

• Whole class or group email addresses for pupils will be used at Ernesford Grange for communication outside of the school.

• Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

• Pupils must immediately tell a teacher if they receive any offensive e-mail.

• Staff will only use official school provided email accounts to communicate with parents and carers.

• Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be.

How will published content be managed?

• The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

• The Head-Teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

• The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

• Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

• Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

• Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.

How will social networking, social media and personal publishing be managed?

• The school will control access to social media and social networking sites.

• Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

• Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.

• Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.

• All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

• Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

How will filtering be managed?

• The school's broadband access will include filtering appropriate to the age and maturity of pupils.

• If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Coordinator who will then record the incident and escalate the concern as appropriate.

• Any material that the school believes is illegal will be reported to appropriate agencies such as the Police or CEOP. How are other technologies managed? Other technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

• Mobile phones for pupils are not encouraged on school premises. The sending of abusive or inappropriate text messages is forbidden.

• No member of staff should use their personal email address for contact with pupil's, parents or governors on School related matters.

• Staff have been advised on appropriate personal security measures when using the internet or personal mobile phones

How should personal data be protected?

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let

individuals find out what information is held about them. The eight principles are that personal data must be:

• Processed fairly and lawfully

• Processed for specified purposes

• Adequate, relevant and not excessive

• Accurate and up-to-date

• Held no longer than is necessary

• Processed in line with individual's rights

• Kept secure

• Transferred only to other countries with suitable security measures.

Policy Decisions

How will Internet access be authorised?

Internet access to staff and pupils should be allocated on the basis of educational need.

At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.

At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Ernesford Grange cannot accept liability for the material accessed, or any consequences resulting from Internet use.

• The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

• The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.

• Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

• All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).

• The Online Safety Co-ordinator will record all reported incidents and actions on CPOMS.

• The Designated Child Protection Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

• The school will manage Online Safety incidents in accordance with the school discipline/behaviour policy where appropriate.

• The school will inform parents/carers of any incidents of concerns as and when required.

• After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

How will e–Safety complaints be handled?

• Any complaint about staff misuse will be referred to the Head-Teacher.

• All Online Safety complaints and incidents will be recorded by the school, including any actions taken.

• Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

• All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How will Social Media be managed?

• Designated persons will access school website and post material for children with parental consent only.

How will mobile phones and personal devices be managed?

• Mobile phones and personal devices should not be brought into school by pupils, except in exceptional circumstances when an agreement has been made by the pupil's parents/carers and school staff. Pupil phones will be locked away at the start of the day and stored in a lockable container. Phones can be collected by pupils at the end of the day.

• Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Staff will be issued with a school phone where contact with pupils or parents/carers is required (however, in an emergency situation, where children's well-being is concerned, staff may use their own phones if necessary).

• Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team.

• Mobile phones may be used by staff in lessons as part of an educational activity or for IT support in cases such as video-conferencing.

• Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

• If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils?

Consideration must be given as to the curriculum place for teaching Online Safety. This could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever pupils are using the internet.

Useful e–Safety programmes include:

• Think U Know: www.thinkuknow.co.uk

• Childnet: www.childnet.com

• Kidsmart: www.kidsmart.org.uk

• Safe: www.safesocialnetworking.org

• All users will be informed that network and Internet use will be monitored.

• An Online Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.

• Pupil instruction regarding responsible and safe use will precede Internet access. An Online Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.

• Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

• Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

• The Online Safety Policy will be formally provided to and discussed with all members of staff.

• Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

• The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

• All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

• Parents' attention will be drawn to the school's Online Safety Policy in newsletters, the school prospectus and on the school website.

• A partnership approach to Online Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use and information leaflets.

• Further advice will be offered to interested parents/carers.

Monthly online safety newsletters will be sent to parents and will be accessible on the homepage of the school website.

This policy will be reviewed every three years, or earlier, if necessary.

Date to be reviewed: 2022

Headteacher: Ian Taylor

Date: September 2021