Oxenhope CE Primary School

# School Policy for Online Safety

# 2017/2018

| Created By: | Date: | Next Review Date: |
|---|---|---|
| A Jones | 2017/2018 | June 2020 |

# Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Oxenhope CE Primary School we understand the responsibility to educate our pupils on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and camera phones.

# Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety co-ordinator in our school is John Parkin who has been designated this role as a member of the senior leadership team. It is the role of the Online Safety co-ordinator to keep abreast of current issues and guidance through organisations such as BDAT, Bradford Safeguarding Board. CEOP (Child Exploitation and Online Protection), Think You Know, NSPCC and liaising with our School's designated Cyber PCSO.

Senior Management and Governors are updated by the Head/ Online Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy **and PHSCE.**

**Online Safety skills development for staff**

- Our staff receive regular information and training on Online Safety issues in the form of staff meetings, twilights and written correspondence.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know to report the misuse of technology by any member of the school community to the Online Safety co-ordinator or the Headteacher.
- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

**Managing the school Online Safety messages**

- We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The Online Safety policy will be introduced to the pupils at the start of each school year.
- Online Safety rules are displayed next to computers.

**Online Safety in the Curriculum**

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety

- The school provides opportunities within a range of curriculum areas to teach about Online Safety.
- Educating Key Stage 2 pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
- Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critical evaluate materials and learn good searching skills through cross curricular teacher models and discussions.

# Managing the Internet

**Use of the Internet to Enhance Learning:**

- The school internet access is designed for pupil use and includes filtering.
- Pupils are taught what internet use is acceptable and what is not.
- Internet access will be planned to enrich and extend learning activities.
- Staff will preview any recommended sites before use.

- Staff will guide pupils in on-line activities that will support 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.

**Authorised Internet Access**

- The school maintains a current record of all staff and pupils who are granted Internet access.
- Parents are 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 or the support technician via the Headteacher or Online Safety co-ordinator.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up to date on all school machines.

**Social Networking**

The use of public social networking sites (e.g instagram, face book) is not allowed in school.

- 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 are taught not to place personal photos on any social network space.

# Mobile technologies

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Staff are not permitted to use mobile phones / texts during lesson time.
- Currently pupils are not allowed to bring personal mobile devices/phones to school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.

# Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and

good ‘netiquette’. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- 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.
- Access in school to external personal e-mail accounts may be blocked.

# Safe Use of Images

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

**Consent of adults who work at the school**

- Permission to use images of all staff who work at the school is sought on induction.

**Publishing pupil’s images and work**

On a child’s entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).
- This consent form is considered valid for the entire period that the child attends this school. Parents/ carers may withdraw permission, in writing, at any time.

Published content and the school website and learning platform.

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

**Webcams**

- Pupils are alerted to the danger of using web cams as an extension of a chat room. Although this will be highly unlikely at school, pupils need to know the risks involved when using web cams at home.
- Parents are asked to sign and return a consent form for pupil access.
- For aspects of the curriculum teachers may plan to use video conferencing or web cams. Children will always be monitored by a member of staff when these technologies are in use.

**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.

**Managing Emerging Technologies**

Emerging technologies will be examined by the ICT co-ordinator for educational benefit and a risk assessment will be carried out before use in school is allowed.

**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.

**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.
- 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.

# Equal Opportunities

**Pupils with additional needs**
The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules.
However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.
Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

# Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting Online Safety both in and outside of school.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school Online Safety policy via Online Safety training, governor meetings, parents questionnaire
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

**Handling Online Safety Complaints**

- Complaints of Internet misuse will be dealt with by the Online Safety co-ordinator or Headteacher and recorded in the Incident Log.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be reported to the Named Persons for Child Protection.

Pupils and parents will be informed of the complaints procedure.
Pupils are encouraged to inform their teacher or other adults in school regarding anything which makes them feel uncomfortable while using ICT.

**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 Online 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.

Parents

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

**Links to Other Policies**

Health and Safety Policy.
Child Protection and Safeguarding Policy.
Acceptable Use Policy.
Anti-Bullying Policy.
P.S.H.C.E.

# Reviewing this Policy

**Review Procedure**

There will be an on-going opportunity for staff to discuss with the Online Safety coordinator any issue of Online Safety that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Reviewed June 2019
Next review June 2020