Online Safety Policy 2017

For review 2020

This policy applies to all staff, pupils, governors and visitors accessing the Internet or using technological devices on school premises. This includes staff or pupil use of personal devices such as mobile phones or iPads, which are brought into school. This policy is also applicable where staff have been provided with school issued devices for use off site such as laptop or mobile phone.

Introduction

The use of information and communication technology is an integral part of the National Curriculum (NC) and is a key skill for everyday life. Computers, iPads, programmable robots, and video cameras are a few of the tools that we use to acquire, organise, store, interpret and communicate and present information. We recognise that pupils are entitled to quality hardware and software and a structured and progressive approach to learning the skills that are needed. Whilst technology has many benefits, we recognise that clear procedures for appropriate use and education, for staff as well as students, about online behaviours, age restrictions and potential risks is crucial.

Aims

- To educate staff, pupils and parents about the pros and cons of using new technology both within, and outside of, the school environment;
- To develop links with parents/carers and the wider community to show awareness of the benefits and potential issues related to technology;
- To teach the children how to use the internet safely;
- To show what procedures the school have in place to safeguard and protect children using the Internet.

Why is Internet use important and what are the benefits to the school?

- It gives pupils immediate access to a rich source of materials;
- It means they can present information in new ways, which helps pupils understand and use it more readily;
- It can motivate and enthuse pupils;
- It has the flexibility to meet the individual needs and abilities of each pupil;
- It offers the potential for effective group working;

- It is a part of the statutory curriculum;
- It enhances the school's management information and business administration systems;
- Information and cultural exchanges can be made between pupils world wide;
- It allows for discussion with experts in many fields for pupils and staff;
- It enables staff professional development- access to educational materials and good curriculum practice.

How will Internet use enhance learning?

- Pupils will be taught what internet use is acceptable and what is not and be given clear rules to adhere to;
- Pupils will also be educated in taking responsibility for what Internet they access;
- Staff will select sites which will support the learning outcomes planned for pupils' age and maturity;
- Internet access will be planned to enrich and extend learning activities.

How will pupils be taught to assess Internet content?

- Pupils will be taught ways to validate information before accepting its accuracy;
- Pupils will be taught to acknowledge the source of information, when using Internet material for their own use;
- Pupils will be made aware that the writer of an email or the author of a web page might not be the person they claim to be;
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that they feel is inappropriate or that makes them feel uncomfortable;
- Pupils will be taught to recognise and deal with SPAM mail.

How will the Internet be managed?

E-mail

- Pupils must only use approved e-mail accounts on the school system for educational purposes;
- Pupils will not be allowed to access personal e-mail accounts from the school system;
- Pupils may send e-mails as part of planned lessons but will not be given an individual e-mail account;
- Pupils must not reveal personal information about themselves or others in e-mail communication or arrange to meet up with anyone;
- Pupils must tell a teacher if they receive any offensive e-mails;
- An e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- The school provides all staff with a professional email account to use for all school related business;
- All emails, should be professional in tone and checked carefully before sending;
- Staff should inform the IT co-ordinator or head teacher if they receive an offensive or inappropriate e-mail via the school system.

Authorising Internet access

- At Key Stage 1, the majority of access to the Internet will be by teacher or adult demonstration. However there may be situations where children have supervised access to specific approved online materials. The use of child friendly applications such as 'youtube for kids' na 'swiggle' will also be encouraged;
- At Key Stage 2, Internet access will be granted to a whole class as part of a scheme of work after a suitable education in responsible Internet use;
- Parents will be informed that pupils will be provided with supervised Internet access, although they must agree by ticking and signing the 'General Permissions form;'
- Children will also be asked to sign a permission form to say that they will adhere to the rules of using the Internet safely and for its intended use;
- Children who are using the Internet will be supervised appropriately.

Published content and the school website

- The contact details on the website are the school address and telephone number as well as the head teacher's email address. Staff or pupil's personal information will not be published;
- Expression of preference for photographs is sought (Photograph policy on school website) and the school ensures named or unnamed photographs are not published on the website if this preference has been given. On each class noticeboard, is a list of children whose name or photograph is not permitted onto the school website.

Social networking and personal publishing

- The school will block/filter social networking sites;
- Pupils will be taught what sites are appropriate for their age group and the dangers of using social media websites and gaming websites with an age restriction;
- Parents will be advised that the use of social networking is inappropriate for primary aged pupils.

Filtering

- Internet access is purchased from a supplier that provides a service designed for pupils. This includes filtering appropriate to the age of the pupils;
- The IT co-ordinator will ensure regular checks are made to ensure that filtering methods are effective;
- If staff or pupils discover an unsuitable site, it must be reported to the IT co-ordinator lead who will then record it in Appendix 4 and report to the IT technician;
- Any material that the school suspects is illegal will be referred to the Internet Watch Foundation (Appendix 3);
- Emails will be filtered and accessed through the Schools Broadband to provide security and protection for the children;
- All users have unique usernames to access the school network, this ensures that they receive the appropriate level of filtering;
- Virus protection will be reviewed and updated regularly.

Managing emerging technologies

- Emerging technologies will be examined by adults for educational benefit and assessed before use in school is allowed;
- Mobile phones will not be used in lessons or formal school time. They will be handed to the class teacher at the start of the school day and returned before home time. Throughout the day, mobile phones should be locked away where only the adult in charge can have access to them;
- Staff mobile phones are permitted onto school grounds although it is the responsibility of the staff member to ensure that there is no inappropriate content stored on their device when brought onto school grounds.

What are the risks of using the Internet and how will this be dealt with?

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 NCC can accept liability for the material accessed, or any consequences thereof;
- 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 Head teacher will ensure that the policy is implemented effectively.

Maintenance of the school's security system

- Security strategies will be discussed with PDET;
- The IT co-ordinator will ensure that the system has the capacity to take increased traffic caused by Internet use;
- The security of the whole system will be reviewed by the IT Co-ordinator and technician with regard to threats to security from Internet access;
- Personal data sent over the Internet will be encrypted or otherwise secured;
- Virus protection will be installed and updated regularly;
- Use of e-mail to send attachments such as system utilities will be reviewed.

Misuse of the Internet

- In the event of minor or accidental misuse, internal investigations should be initiated and procedures should follow appropriately;
- All security breaches, lost/stolen equipment or data, or misuse of the Internet should be reported immediately to the head teacher, who will log the information on the Online Safety Incident Log (Appendix 5) and follow the necessary procedures;
- Responsibility for handling incidents will be given to the Head Teacher;
- Any complaint about staff misuse must be referred to the Head teacher;
- Sanctions may involve being interviewed or receive counselling by the Head Teacher, and, if appropriate, informing parents and carers;

- Parents and pupils will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues;
- A pupil may have internet or computer access denied for a period of time depending on the nature of the incident;
- If there are any occasions when the police must be contacted, early contact will be made to establish legalities and to discuss strategies to move forward;
- Complaints of a Child Protection nature are dealt with in accordance with the School's Child Protection Procedures.

Introducing the E-safety policy to staff, pupils and parents

- E-safety rules will be posted in all networking areas and discussed with pupils at the start of each term;
- Pupils will be informed that their Internet use will be monitored;
- Pupils are encouraged to report any material they find distasteful, uncomfortable or threatening to their class teacher;
- All staff members will be provided with the Online Safety policy, have its importance explained, as well as signing Appendix 1;
- Staff will be kept up to date by the IT co-ordinator with new any new changes to the policy and any changes linked to e-safety in schools;
- Staff will be educated about new technology and any implications they have in school through staff meetings;
- Parents' attention will be drawn to the policy through the use of the school's website and when opportunities arise for outside agencies to talk to parents;
- Pupils will be taught to adopt safe and responsible practices when using new technology through PSHE, IT lessons and an age appropriate curriculum alongside the assistance of outside agencies;
- If a pupil has a specific learning requirement, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness and Internet access.

Responsibilities

IT co-ordinator/ Technical staff must ensure that:

- The school's infrastructure is secure and not open to misuse;
- The anti virus software is installed and maintained on all school machines;
- The school's filtering policy is applied and updated on a regular basis and a log of any changes must be updated on the Filtering Change Log (Appendix 4);
- They keep up to date with e-safety technical information in order to maintain the security of the schools network and to safeguard pupils;
- Staff are kept up to date with any new changes with regards to e-safety in school;
- Regularly audit the training needs for staff and provide training to improve knowledge and expertise.

Children must ensure that:

- They read and sign the document Rules for Responsible Use (Appendix 2) and abide by the appropriate rules set out in the document;
- They use the internet and technology in a safe and responsible manner within school, which shall be taught and reinforced by class teachers;
- They inform staff of any inappropriate material or cyber bullying they come into contact with. Staff members should then record this onto the Online safety incident log (Appendix 5).

Parents must ensure that

- They read the Acceptable Use Rules on an annual basis or first time entry to the school;
- They try to attend any e-safety sessions that are run to increase their knowledge of key Internet safety issues;
- They encourage their child/children to talk about what they have been doing on the Internet and to discuss any issues that they may find upsetting.

Appendix 1
Isham CE Primary School

Acceptable Internet Use Statement for Staff

The computer system is owned by the school and is made available to students to further their learning 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.
Staff requesting Internet access should sign a copy of the Acceptable Internet Use Statement and return it to the ICT Co-ordinator.

- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Copyright of materials must be respected;
- All Internet activity should be appropriate to staff professional activity or the student's education. Legitimate private interests may be followed where these cause no difficulties for other users and do not compromise school use;
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mails are often forwarded or may be sent inadvertently to the wrong person;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Users must access only those sites and materials relevant to their work in school. Users will be aware when they are accessing inappropriate materials and should expect to have their permission to use the system removed.

Full name …. … … … … … … … … … Post … … … … … … … … … …

Signed … … … … … … … … Date … … … … … …

Access granted … … … … … … … … Date … … … … … …

Appendix 2
Isham CE Primary School

Pupils' Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will not access other people's files;
- I will only use the computers for school work and homework;
- I will ask permission from a member of staff before using the Internet;
- I will only e-mail people whom I know, or my teacher has approved;
- The messages I send will be polite and sensible;
- I will not reveal any information about myself or others;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

Signed: Class:

Appendix 3

References

Particularly for Parents:

Government site for Parents Information about education for parents
www.dfee.gov.uk/parents

NCH Action for Children. A Parents'Guide to the Internet leaflet. www.nchafc.org.uk/internet

Parents and IT. BECTa information sheet. www.becta.org.uk/info-sheets/parents.html

Parents' Information Network(PIN).Guidelines on using the Internet safely. www.pin-parents.com

Superhighway Safety Pack
http://vtc.ngfl.gov.uk/vtc/library/safety.html

Free pack from DfEE on safe Internet use Tel: 0845 6022260

Particularly for Schools:

Association for Co-ordinators and Teachers of IT (ACITT. Acceptable Use Policy for UK Schools.
www.acitt.org.uk/aup.html

Connecting Schools, Networking People 2000
BECTa, October 1999 (free order line) Tel: 024 7641 6669

Kent NGfL Website. Latest version of this policy. www.kent.gov.uk/ngfl/policy.html

Internet Watch Foundation www.iwf.org.ukReporting
Illegal Internet material Tel: 0845 600 8844.

Irish National Centre for Technology in Education. Comprehensive advice on Internet use
www.ncte.ie/support.htm

Promoting the Responsible Use of the Internet in Schools. British Computer Society / NAACE
www.bcs.org.uk/iap.htm

The Internet and the World Wide Web. Information sheet published April '99
www.becta.org.uk/info-sheets/internet.html

Appendix 4
Filtering change log

Website	Date	Reason	Requested by	Change made by	Date

Appendix 5
Online Safety Incident Log

Date of incident	Individuals involved	Device number/location	Details of incident	Action taken	Confirmed by