ICKFORD SCHOOL

E-Safety Policy

October 2022

Introduction

At Ickford School we understand the responsibility we have to educate our pupils on e-safety issues; teaching them 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.

Ickford School has a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:
- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive e-safety programme for pupils, staff and parents.

This policy has been contributed to by the whole school and ratified by the Trustees.

This policy is to be read in conjunction with all other policies particularly: Behaviour Policy, Child Protection Policy, Code of Conduct policy, and Equal Opportunities Policy.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in Ickford School. All staff have received Child Protection Awareness Training and Prevent training. The Headteacher has overall responsibility and staff and children are to report any concerns to him.

It is the role of the Headteacher to keep up to date with current issues and guidance. The Head teacher also ensures Senior Management and Trustees are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:

• safe use of e-mail
• safe use of the Internet
• safe use of the school network, equipment and data
• safe use of digital images and digital technologies, such as mobile phones and digital cameras
• publication of pupil information/photographs on the school website
• procedures in the event of misuse of technology by any member of the school community (see appendices)
• their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign a staff internet code of practice agreement before using technology equipment in school (see appendix 2 for staff internet code of practice).

Managing the school e-safety messages

• We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.

• The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.

• E-safety posters will be prominently displayed.

Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new ways to promote e-safety.

• We provide opportunities within a range of curriculum areas to teach about e-safety.
• Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.
• Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.
• Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
• Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people.

Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use.

The school firewall (Fortinet) restricts access to potential harmful websites.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, it is advised that parents recheck these sites and supervise any further research.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator and an email sent to Wibird the school's IT support so that they can block the site.

It is the responsibility of the school, by delegation to Wibird, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Any changes to filtering must be authorised by a member of the senior leadership team.

Security and Data Protection

The school and all staff members comply with the Data Protection Act 2018. Personal data will be recorded, processed, transferred and made available according to the act. Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have secure passwords which are not shared with anyone. All users read and sign a staff internet code of conduct acceptable to demonstrate that they have understood the school's E-Safety Policy.

E-Safety Complaints/Incidents

As a school we take all precautions to ensure e-safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Headteacher. Incidents should be logged and the complaints policy should be followed. It is important that the school work in partnership with pupils and parents to educate them about Cyber bullying and children, staff and families need to know what to do if they or anyone they know are a victim of Cyber bullying. All bullying incidents should be recorded and investigated.

Review of Policy

There are on-going opportunities for staff, children and families to discuss e-safety concerns. This policy needs to be reviewed every 12 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or any guidance or orders are updated.

Appendix

1. Pupils Internet Code of Practice
2. Staff Use of Internet Form
3. Advice for children on Cyber Safety

Appendix 1

Pupil's Internet Code of Practice

- Pupils must only use the internet in school with permission and under the supervision of an adult
- Pupils must not give out any personal details over the Internet unless their teacher and parents have given permission
- Pupils must not send pictures of themselves or friends over the Internet
- Pupils must not access chat rooms or social networking sites
- Pupils must not attempt to access gaming or gambling websites
- Pupils must not send emails without the permission of a teacher
- Pupils must not send emails that contain bad language or nasty comments about other people
- Pupils must not forward chain messages
- Pupils must always report anything that they find upsetting on the Internet to their teacher or another adult
- Pupils must not download any material from the Internet without the permission of a teacher
- Pupils must report anything that makes them feel uncomfortable to a teacher or other adult immediately
- Pupils must not download material from any storage device without the permission of a teacher
- I accept that if my child misuses the Internet they will be prevented from further use in school
- I accept that misuse of the Internet may result in sanctions for my child
- Pupils must not participate in any activity that may incite religious intolerance

I have read the Pupil's Code of Practice and I have discussed it with my child. We agree to support the school's policy on the use of the Internet.

Signed……*(Parent/Guardian)*

Child's name ……

John Ronane

HEADTEACHER

Appendix 2

Staff Internet Code of Practice

- Staff should be familiar with the school's Network, internet, email and website creation policies and the pupils' code of practice for internet use.
- Teachers should closely monitor and scrutinise what their pupils are accessing on the internet including checking the history of pages.
- Computer monitor screens should be readily visible for the teacher, so they can monitor what the pupils are accessing.
- Pupils should have clear guidelines for the content of email messages, sending and receiving procedures.
- Use of the internet should be supervised by a teacher or adult.
- Pupils should be taught skills and techniques to enable efficient and effective use of the Internet.
- Pupils have a clearly defined focus for using the internet and email.
- If offensive materials are found, the monitor should be switched off, any printed materials or disks should be confiscated and offensive URLs should be given to the IT Co-ordinator who will report it to the Internet Service Provider.
- Virus protection has been provided by the school as viruses can be down loaded accidentally from the Internet. Pupils bringing work from home, on floppy disk, or memory stick, could also infect the computer – some viruses will format your hard disc.
- The recommended ISP will check sites visited by schools.
- It is recommended that pupils do not use open forums such as newsgroups or chat rooms.
- Disciplinary action may be taken if the internet is used inappropriately, e.g. for accessing pornographic, racist, or offensive material for personal financial gain, gambling, political purposes or advertising.
- Software should not be downloaded from the Internet (including screen savers, games, video clips, audio clips, *.exe files).

I have read the Code of Practice for pupils and staff and I am familiar with the school's policy on the use of the internet, email, the creation of web sites and network security.

I agree to abide by these policies and the Staff Internet Code of Practice.

Name: ……..

Signed: ……..

Date: ……..

Appendix 3

Key Safety Advice

The whole school community has a part to play in ensuring cyber safety. Understanding children and young people's online lives and activities can help adults respond to situations appropriately and effectively. Asking children and young people to show adults how technologies and services work is a useful strategy that can provide an important learning opportunity and context for discussing online safety.

For children and young people

1: Always respect others – be careful what you say online and what images you send.
2: Think before you send – whatever you send can be made public very quickly and could stay online forever.
3: Treat your password like your toothbrush – keep it to yourself. Only give your mobile number or personal website address to trusted friends.
4: Block the bully – learn how to block or report someone who is behaving badly.
5: Don't retaliate or reply!
6: Save the evidence – learn how to keep records of offending messages, pictures or online conversations.
7: Make sure you tell:
- an adult you trust, or call a helpline like ChildLine on 0800 1111 in confidence;
- the provider of the service; check the service provider's website to see where to report incidents;
- your school – your teacher or the anti-bullying coordinator can help you.

Finally, don't just stand there – if you see cyberbullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?

For parents and carers

1: Be aware, your child may as likely cyberbully as be a target of cyberbullying. Be alert to your child seeming upset after using the internet or their mobile phone. This might involve subtle comments or changes in relationships with friends. They might be unwilling to talk or be secretive about their online activities and mobile phone use.
2: Talk with your children and understand the ways in which they are using the internet and their mobile phone. See the seven key messages for children (on the left) to get you started.
3: Use the tools on the service and turn on in-built internet safety features.
4: Remind your child not to retaliate.
5: Keep the evidence of offending emails, text messages or online conversations.
6: Report cyberbullying:
- Contact your child's school if it involves another pupil, so that they can take appropriate action.
- Contact the service provider.
- If the cyberbullying is serious and a potential criminal offence has been committed, you should consider contacting the police.