ICKFORD SCHOOL

Online Safety Policy

September 2025

Introduction

At Ickford School we understand the responsibility we have to educate our pupils on online safety; 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 online safety programme for pupils, staff and parents.

This policy has been contributed to by the whole school and ratified by the Trustees.
This policy aligns with statutory guidance in *Keeping Children Safe in Education 2025* (KCSIE), *Teaching Online Safety in Schools* (DfE 2019, updated 2023), and uses the nationally recognised "4Cs" framework of online risk: Content, Contact, Conduct, and Commerce.

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

Roles and Responsibilities

Online Safety is led by the Headteacher/Designated Safeguarding Lead (DSL), who has overall responsibility for online safety as part of their safeguarding role. The DDSLs support the DSL, and Trustees have strategic oversight including responsibility for ensuring appropriate filtering and monitoring systems are in place and reviewed.

All staff have received Child Protection Awareness Training, Prevent training, and regular updates on online safety as part of safeguarding training.

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 online safety education for pupils.

Supply teachers and visiting staff must sign the staff acceptable use agreement before using school technology.

Managing the School's 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 shared with new staff, including the acceptable use policy as part of their induction.
• Posters and pupil-friendly materials will be displayed around the school, not just in ICT rooms, to reinforce safe behaviour.

Curriculum

Computing 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.
• We provide opportunities within a range of curriculum areas to teach about online safety, including through RSHE and external visits.
• The school follows the "Education for a Connected World" framework to ensure age-appropriate coverage.
• Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities.
• Pupils are taught about online bullying (in place of "cyber bullying") through PSHE/RSHE and know how to seek help if they are affected by these issues.
• Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies, including external reporting routes such as CEOP, Childline and the Internet Watch Foundation.
• Pupils are taught to critically evaluate materials, recognise misinformation and fake news, and learn good searching skills through cross-curricular teacher models and discussions.
• Pupils are taught about healthy online behaviours including screen time, privacy, respect and consent in online relationships, and commercial risks such as scams and in-app purchases.

Managing Internet Access

The internet poses potential risks to young people. Pupils will have supervised access to internet resources through the school's fixed and mobile internet technology.
• The school firewall (Fortinet) restricts access to potentially harmful websites (set up through Wibird).
• If unsuitable sites are discovered, the screen must be closed and the incident reported immediately to the DSL and IT support.
• Any changes to filtering must be authorised by a member of the senior leadership team.
• Filtering and monitoring systems are reviewed termly by the DSL and reported to trustees to ensure they are effective, age-appropriate and in line with DfE standards (2023).

Security and Data Protection

The school and all staff comply with the UK GDPR and the Data Protection Act 2018.
• Staff have secure passwords which are not shared with anyone.
• All staff and pupils sign acceptable use agreements to confirm understanding of safe practice.

• When using online platforms (e.g. for homework or remote learning), only systems compliant with data protection and safeguarding standards will be used.

Online Safety Complaints/Incidents

As a school we take all precautions to ensure online safety at all times. However, due to the nature of the internet and mobile technologies, unsuitable material may occasionally appear.
• Concerns or complaints should be reported to the DSL (or Headteacher in their absence).
• Incidents are logged and managed under safeguarding and complaints procedures.
• Children will always be supported as potential victims first — sanctions will not be applied in a way that discourages reporting.
• All bullying incidents, including **online bullying**, are recorded and investigated in line with the Behaviour and Anti-Bullying Policy.
• External reporting routes (CEOP, IWF, NSPCC/Childline) are shared with pupils and families.

Remote Learning and Emerging Risks

The school recognises that online learning, live-streaming, AI tools and emerging technologies present additional safeguarding risks. Staff follow professional guidance during remote or online sessions. Pupils are educated about the safe and responsible use of AI tools, recognising bias, misinformation and age restrictions. Trustees and the DSL will ensure risk assessments are carried out for any new digital tools introduced.

Review of Policy

There are ongoing opportunities for staff, children and families to discuss online safety concerns. The policy will be reviewed annually by the DSL and Trustees, with particular reference to the effectiveness of filtering and monitoring, curriculum coverage, and emerging risks.
Amendments will be made in line with new technologies, statutory updates or safeguarding guidance.

Appendices

Appendix 1 – Pupil 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 personal details unless approved by a teacher and parent.
• Pupils should be cautious about sharing images online and understand when it is unsafe to do so.
• Pupils must not access age-inappropriate websites, gaming or gambling platforms.
• Pupils must always use respectful language online.
• Pupils must report anything that upsets them or makes them feel uncomfortable to a teacher or trusted adult immediately.
• Pupils are encouraged to use safe reporting tools such as CEOP or Childline with adult support.
• I accept that misuse of the internet may result in sanctions in line with the Behaviour Policy.

Parent/Guardian signature: _____
Child's name: _____

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.