Online Safety Policy
2026 - 2027

Headteacher	Anita Spires
Chair of Governors	Katherine Russell
Date ratified by LGB	October 2026
Renewal date	October 2027

Contents Page

Introduction 2

Aims 3

Roles and Responsibilities 4

- Online Safety Officer 4
- IT Staff 4
- All Students 4
- Parents and Carers 5

Raising Awareness 5

Accessing the Internet on School premises: Monitoring and Filtering 5

- Impero 5
- Internet Filtering 5
- Passwords 6
- Anti-Virus 6
- FastVue 6
- Ems 6
- Printing Facilities 6

Legislation and Guidance 6

Online Safety Tips 7

Useful Websites 7

Appendix 1: Online Safety Policy Agreement Proforma 8

Online Safety Policy

Introduction

Beechwood School has a positive policy of equality and diversity and strives to support students wherever possible. The school also has a duty of care to safeguard all of its stakeholders including staff, students and visitors and is committed to providing a safe environment for study and work.

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation; radicalisation and sexual predation. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, racist or radical and extremist views, and in some respects fake news.
- **Contact:** being subjected to harmful online interaction with other users; for example, children can be contacted by bullies or people who groom or seek to abuse them.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the school's environment. Current and emerging technologies of the school and more importantly, in many cases used outside the school by students, include (but are not limited to):

- Internet websites
- Instant messaging
- Social networking sites
- E-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- Smart phones, iPads and Tablets with e-mail and web applications.

Aims

- To ensure that everyone who works and learns at the school achieves their full potential safely in an environment free from discrimination.
- To have procedures that take account of an individual's right to education balanced by the risk to the school and its wider community.
- To prepare students for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies.
- To provide guidance on the safe and acceptable use of Online Technologies including social media communications, by students inside and outside of the school.

Roles and Responsibilities

Online Safety Officer

The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the Head.

- Advise the Head and Governing body on all Online Safety matters.

- Liaise with the DSL to engage with parents and the school community on Online Safety matters at school and/or at home.

- Retain overall responsibility for Online Safety incident reporting

- Ensure any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.

- Make him/herself aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the Head and responsible Governor to decide on what reports may be appropriate for viewing.

IT Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  - Antivirus is fit-for-purpose, up to date and applied to all capable devices.
  - Software updates are regularly monitored and devices updated as appropriate.
  - Any online safety technical solutions such as Internet filtering are operating correctly.
  - Filtering levels are applied appropriately to all areas.

All Students

- Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- Online Safety is embedded into the curriculum students will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum.
- All students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have access to resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school bulletins and the availability of free online training courses the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such all new Year 7 and in -year transition parents will sign the Online Safety Policy before their child can be granted any access to school network, ICT equipment or services.

We have a digital detox in place across the school day for all students in Years 7-11. Mobile devices are handed in and stored safely during school hours.

Raising Awareness

- Online safety awareness is delivered throughout the year, to all students during dedicated lessons throughout the year - for example sessions that focus on online reputation, exploitation, online gaming and sleep awareness.

- Online E-safety evenings are run for parents and carers with the aim of educating and guiding with reference to the importance of e-safety both inside and outside of the home.

- Students are expected to adopt an attitude of 'collective responsibility' towards online safety by encouraging others to stay safe and report any concerns to a member of Beechwood staff.

- Regular training is provided for all staff in regards to online safety, safeguarding, sexual and criminal exploitation and radicalisation.

Accessing the Internet on School premises: Monitoring and Filtering

Beechwood School uses a range of devices including PC's, and laptops. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Impero

Impero Education Pro combines learner wellbeing and device management to enhance digital learning, support IT administration and monitor safeguarding issues effectively.

Internet Filtering

The WebBlocker prevents unauthorised access to illegal websites, including those sites deemed inappropriate. WebBlocker uses content categories to group different websites. A website is added to a category when the content of the website meets the criteria for the content category. Web access is logged for all users of the IT systems in Beechwood School.

WebBlocker may block access to some sites; if such a site is related to a student's normal working requirements contact a teaching member of staff who will contact IT Helpdesk to arrange for the site to be reviewed and unblocked (where permissible).

Passwords

All students will be unable to access the network without a unique username and password. Student passwords should be changed if there is a suspicion that it has been compromised. The use of another person's credentials at any time is forbidden.

Anti-Virus

All capable devices will have anti-virus software. This software will be updated daily for new virus definitions.

FastVue

FastVue is a device-level software which reports on all internet activity undertaken on any device located in the school. Daily reports are sent to the IT team which are checked for any violations and any safeguarding issues are reported to the Safeguarding Officer

Ems

EMS is software which allows the school to filter Chromebooks irrespective of whether they are in school or used purely at home. This results in the same WebBlocker as provided in school thus preventing staff and pupils from accessing illegal websites, including those sites deemed inappropriate.

Printing Facilities

Each student's print account will be tracked through the print management software. Printing credit is intended for school use only. If it has been highlighted that a student has used the printing facilities to print inappropriate items or has been used for personal use, without prior permission being sought, they may be liable for those printing costs. All student accounts will be provided with a set amount of credit at the beginning of each month. Students who exceed their print credit must inform the teaching staff that they have run out of credit for IT to action accordingly.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying for headteachers and school staff
- Searching, screening and confiscation
- Protecting children from radicalisation

Please find here to Beechwood School's Safeguarding Policy.

Online Safety Tips

Always think of your personal safety first when using IT or your mobile phone.

- Remember it is easy for anyone to lie about who they are online, so you can never really be sure about who you are talking to.

Do not give out any personal information about yourself online to people you do not know.

- This includes your full name, address, street name, postcode or school name.

Always remember, what goes online, stays online.

- Just because you might have deleted a message, photo or video, does not mean that someone hasn't copied it beforehand. Think about whether you might want potential future employers seeing it?

Don't meet people who you have only spoken to online.

- They could have a fake profile and not be who they say they are.

Don't be persuaded to send personal photos of yourself to anybody.

- You may think this person can be trusted but they may pass this image to someone else. It is easy for people to take your pictures and alter them, send them on, or even pretend to be you with them.

Always use private settings whenever you are setting up a social networking page or an Instant Messenger (IM) account.

- This is so people who you don't want to see your profile can't.

Think about what information your photos give away.

- Do your photos show what school you go to, where you live, where you 'hang out'? You might not realise it but photos give away a lot of information about you.

Never go onto webcam with people you don't know in real life.

- Webcam images can be recorded and copied and also shared with other people.

If you receive any messages or pictures that worry or upset you, talk to an adult you trust.

- You may also report it online via the website www.thinkuknow.co.uk or NSPCC – https://www.nspcc.org.uk

Useful Websites

- Child Exploitation and Online Protection Centre https://www.ceop.police.uk
- UK Safer Internet Centre https://www.saferinternet.org.uk/
- CEOP's Think You Know https://www.thinkuknow.co.uk/
- Net Aware https://www.net-aware.org.uk/
- Internet Watch Foundation https://www.iwf.org.uk/

Appendix 1

Online Safety Policy Agreement

We have an Online Safety Policy Agreement in place to safeguard children in their use of technologies such as the internet, mobile phones, digital devices, etc. We want to ensure that:

- Children will be responsible users and stay safe while using the internet and other communication technologies (for educational, personal and recreational use)
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents/carers are aware of the importance of Online Safety and are involved in the education and guidance of their children with regard to their online behaviour.

The school will ensure that our students have good access to ICT to enhance their learning and expect that they agree to be responsible users.

As the parent/carer of a student at Beechwood School, I:

- Understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems.
- Understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- Understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have any concerns about possible breaches of the Online Safety Policy Agreement.
- Encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Child's Name (printed): _____

Parent/Carer Name (printed): _____

Signature: _____

Date: _____