



Online Safety Policy

1. Statement

1.1. This policy applies to the whole School, including EYFS. It should be read in conjunction with the Safeguarding & Child Protection Policy, Anti-Bullying Policy, Behaviour & Exclusion Policy, relevant Privacy Notices along with policies for staff including the Code of Conduct, Staff Handbook, IT Acceptable Use Policy – Staff, and Disciplinary Policy.

1.2. It is essential that children are safeguarded from potentially harmful and inappropriate online material. The breadth of issues classified within online safety is considerable and ever evolving but can be categorised into four areas of risk

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children, or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example: making, sending or receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Introduction and aims

2.1. Computing is an integral part of the way the School works, is a crucial component of every academic subject and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the School.

2.2. Nearly all of the teaching areas are equipped with CLEVERTOUCH boards and computers. The School has a Computing suite and pupils may use the machines there and elsewhere for private study if supervised. The School also has mobile internet-connected devices for use in the classroom and grounds.

2.3. This policy aims to:

- Set guidelines and rules on the use of School computing resources for staff, pupils, and parents
- Establish clear expectations for the way all members of the School community engage with each other online
- Support the School's policy on data protection, online safety and safeguarding
- Prevent disruption to the School through the misuse, or attempted misuse, of computing systems
- Support the School in teaching pupils safe and effective internet and computer use

3. The role of technology in our pupil's lives

3.1. Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles, or PSPs (play stations portable), like Wiis and Nintendo DS, together with Bluetooth-enabled mobile phones provide unlimited access to the internet, to SMS messages, to blogging (web logging) services (like Twitter), to Teams and Zoom (video calls, via web cameras built into computers, phones and PSPs) to wikis (collaborative web pages), chat rooms, social networking sites (such as Facebook, TikTok, Snapchat and Instagram) and video sharing sites (such as YouTube).

3.2. This communication revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the role of Ripley Court to teach pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. Pupils also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

3.3. Within the explosion in technology, the School recognises that blocking and barring sites is no longer adequate. Pupils need to be taught to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for the IT Department, the DSL and the Pastoral Staff.

3.4. The IT Department have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of the hardware, system, the data and for training teaching and administrative staff in the use of computers. They monitor the use of the internet and emails and will report inappropriate usage to the DSL.

4. Role of our Designated Safeguarding Leads (DSL)

- 4.1. The School recognises that internet safety is a child protection and general safeguarding issue. The DSLs have been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices.
- 4.2. The Headmaster is the Designated Safeguarding Lead. The role of Online Safety Co-ordinator is held by Pippa Moody. The DSLs and Deputy DSLs work closely with the relevant external agencies as required, in promoting a culture of responsible use of technology consistent with the ethos of the School.
- 4.3. Relevant staff receive training in e-safety issues. The school has a comprehensive Personal Social Health and Economic (PSHE) Education programme and this, together with support from the IT Department, aims to ensure that all year groups in the School are educated in the risks and the reasons why they need to behave responsibly online.
- 4.4. The School has a risk assessment that considers and reflects the risks that pupils face. This helps inform our policy and practices. This risk assessment is reviewed at least annually. An annual review of our approach to online safety is carried out using 360Safe.

5. Misuse: Statement of Policy

- 5.1. The School will not tolerate any illegal material, and will always report illegal activity to the Police and/or other external agencies in line with its Safeguarding & Child Protection Policy.
- 5.2. If staff discover that a child or young person is at risk as a consequence of online activity, the School may seek assistance from the Child Exploitation and Online Protection Unit (CEOP) whilst at the same time making sure our response recognises the needs and support of the person experiencing the abuse.
- 5.3. The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy and our Behaviour, Sanctions and Exclusions Policy. This may include exclusion. Pupils are expected to follow the Charter for the safe use of technology (See Appendix A). Parents/guardians are expected to support the School and their child in ensuring that pupils follow the Charter.
- 5.4. All pupils at Ripley Court School have a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Ripley Court is strongly committed to promoting equal opportunities for all, regardless of race, religion, gender, gender orientation or physical disability.

6. Involvement with Parents/Guardians

- 6.1. The School seeks to work closely with parents/guardians in promoting a culture of online safety. Staff will always contact a child's parents/guardians if there are any

concerns about a child's behaviour in this area. The School hopes that parents/guardians will feel able to share any worries with staff.

6.2. The School recognises that not all parents/guardians feel equipped to protect their child when they use electronic equipment at home. Advice to parents/guardians on the potential hazards and practical steps that can be taken to minimise the potential dangers to children, without curbing their natural enthusiasm and curiosity, are available from staff upon request.

6.3. Parents, and Year 4 and above pupils, are asked to sign an Acceptable Use Agreement. This form can be found in Appendix 1.

7. Communicating with or about the School online

7.1. The School believes it is important to model excellent standards for pupils, and help them to learn how to communicate respectfully with, and about, others online.

7.2. Parents play a vital role in helping model this behaviour for their children, especially when communicating with the School through our website, email and social media channels.

8. Pupil access to Computer Equipment

8.1. Computers and iPads are available to pupils only under the supervision of staff. Computers are password protected and pupils are provided with this information by their teacher. Staff have the ability to lockdown iPads when a guided task is required. This password is not shared with pupils.

8.2. The School discourages pupils from bringing mobile phones and other electronic devices into School on a regular basis unless this has been agreed with the Headmaster.

9. Internet Access

9.1. The School's wireless internet connection is secured. Filtering is provided by an external company and is managed by the SLT in conjunction with the IT department. School devices are connected to the secure wifi port, with a guest login available for all other instances. Inaccuracy of filtering or inappropriate site access should be immediately reported to the IT department.

9.2. Pupils will not have access to wifi through personal devices, only school provided devices. Wifi passwords must not be shared with pupils.

9.3. Parents will not be permitted to use the School's wifi unless specific authorisation is granted by the SLT. Permission is only likely to be granted where parents are working with the School in an official capacity (e.g. as a volunteer or as a member of RCPTA).

- 9.4. Visitors who need to access the School's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan) will be provided with a temporary wifi password.

10. Search and Deletion

- 10.1. Under the Education Act 2011, and in line with the current DfE guidance, the School has the right to search pupil's phones, computers or other devices for pornographic images or any other data or items banned under the School's rules.
- 10.2. The School can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the School's rules.
- 10.3. Staff members may also confiscate devices for evidence to hand to the Police, if a pupil discloses that they are being abused and that this abuse contains an online element.

11. Promoting Safe Use of Technology

- 11.1. Children are taught about the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment, radicalisation and identity theft. They understand that adults, children, and adults pretending to be children, can pose a risk to their safety and that they should avoid giving out any personal details about themselves, their school or their family.
- 11.2. Pupils are reminded that the values of "Ready, Respectful, Safe" apply equally to the online world.
- 11.3. The School follows the Jigsaw PSHE Programme where Online Safety is covered as a part of the physical health and mental wellbeing across all the age ranges from Year 1 to Year 6. (Further details can be found in our PSHE/RSE Policy).
- 11.4. Guidance explains that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.
- 11.5. The School also holds an annual online workshop day for all our pupils from Reception to Year 6 delivered by an outside visitor who follows this up on the same day with a webinar for parents/guardians.

12. Safe Use of Personal Electronic Equipment

- 12.1. The School gives guidance to pupils in an age-appropriate way. For example, when discussing online conduct, for our youngest pupils we might give guidance that no one should put anything onto the web that they would not say to their grandmother.

12.2.The School strongly recommends that parents do not allow children onto social networking sites until they are of a suitable age (usually 13/14). The School feels this helps to reduce the chances of children coming into contact with harmful material.

12.3.In addition to the Jigsaw PSHE Programme, which covers Online Safety, our PSHE lessons also include guidance on how pupils can identify the signs of a Cyberstalker, and what they should do if they are worried about being harassed or stalked online.

12.4.The School offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.

12.5.The School gives guidance on how to keep safe at home, by encrypting your home wireless network, not opening unknown attachments and reporting any illegal content.

13. Considerate Use of Electronic Equipment - Children

13.1.With the exception of mobile phones all other personal electronic devices are banned from the School site unless specific permission has been granted by a senior member of staff. Where a child wishes/needs to bring a mobile phone into School, permission must be sought from the Headmaster in advance. This is unlikely to be given unless there is a clear need from a medical or safety perspective. For example, where a pupil travels in a taxi to or from School or to receive medical alerts/reminders.

13.2.Pupils should not wear watches to School which are able to receive or send messages. Should a pupil arrive at School with such an item, this will be confiscated until the end of the school day when it will be returned to the parent/guardian.

13.3.It is expected that all pupils will adhere to these requirements, and that all children at age 9 (year 4) and their parents/guardians are asked to sign an Acceptable Use Policy document.

14. Note for staff and other adults

14.1.Staff and adults are to be very careful in the use of cameras, in particular those on Mobile Phones, which may enable pictures to be sent more easily electronically. Staff must follow the School's "Creating, Using, Sharing & Storing Images of Children Policy" and the "IT Acceptable Use Policy – Staff". Mobile phones should not be left unlocked and unattended and should not be used whilst on duty, unless in an emergency.

14.2.The School requires staff to use a multi-factor authentication system when making use of School systems. This approach enhances security by adding multiple layers of protection, making it significantly harder for unauthorised users to access sensitive information.

Compiled by: Gavin Ryan (Headmaster)	Revision Number: 6 (Autumn Term 2025)
Approved by: Education & Pastoral Committee	Next Revision date: Autumn 2026

Revision History Table

Revision Number	Section/Paragraph number	Amendments
6 – Autumn 2025	Title	Changed from “E-Safety Policy” to “Online Safety Policy”
	Whole document	Change references to “ICT” to “Computing”
	1.1	Update to policy title
	1.2	New
	14.1	Final sentence extended to make clear that mobile phones should not be used whilst on duty unless in an emergency.
	14.2	New
	Appendix A	Deletion of references to pupils use of mobile phones on educational visits.

Appendix A

CHARTER FOR THE SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES AT RIPLEY COURT

Online safety is a whole school responsibility, and at Ripley Court, the staff and pupils have adopted the following charter for the safe use of the internet inside the school:

Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our school's anti-bullying policy describes our preventative measures and the procedures that will be followed when we discover cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe computing environment at school; but everyone needs to learn how to stay safe outside the school.
- We value all of our pupils equally. It is part of our ethos to promote considerate behaviour, and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff and dealt with under the auspices of our anti-bullying policy.

Treating Other Users with Respect

- We expect pupils to treat staff and each other online with the same standards of respect as they would in the course of face-to-face contact.
- We expect a degree of formality in communications between staff and pupils, and would not normally expect them to communicate with each other by text or mobile phones.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Ripley Court is strongly committed to promoting equal opportunities for all, regardless of race, religion, gender, gender orientation or physical disability.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology or worrying issue to a member of the pastoral staff.
- The use of cameras on mobile phones is not allowed.

Keeping the School Network Safe

- Certain sites are blocked by our filtering system and our computer department monitors pupils' use of the network and email traffic.
- We do not issue pupils with their own personal school email address.

- Access to the school system is via secure personal LOGON, which is password protected. We give guidance on the reasons for always logging off and for keeping all passwords securely.
- We have strong anti-virus protection on our network.
- Any member of staff or pupil or guest, who wishes to connect a removable device to the school's network, will have to obtain a password from the Headmaster.
- The use of the network constitutes an agreement to abide by this policy.

Name of Pupil_____

Form:_____

Signature of Parent/Guardian:_____

Signature of Pupil (Year 4 and above):_____