

E-Safety Policy

Colfe's School: Acceptable Use of ICT, Mobile Phones, and Other Electronic Devices Policy

Policy Scope:

This policy applies to the entire Colfe's School community, including the Early Years Foundation Stage (EYFS).

Responsible for Policy:

Designated Safeguarding Lead / Online (E) Safety Lead / Safeguarding Link Governor.

Guiding Principle:

"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool, we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim." - Dr. Tanya Byron, Safer Children in a Digital World: The Byron Review

Review Dates:

Last Review: August 2025

Updated December 2025

Next Review: August 2026

Objectives:

Colfe's School aims to ensure secure access to ICT for all pupils. This policy outlines the acceptable use of internet and electronic communication facilities, file-servers, messaging services, and any networks or hardware, including personal devices and other equipment that can be used to access, store, or record data or media files.

Compliance with UK Legislation:

This policy is in compliance with the following UK legislation and guidance:

Data Protection Act 2018 (DPA 2018)

General Data Protection Regulation (GDPR)

Education Act 2011

Keeping Children Safe in Education (KCSIE) 2025

The Prevent Duty 2015

The Equality Act 2010

The Communications Act 2003

The Computer Misuse Act 1990

The Human Rights Act 1998

The Children and Families Act 2014

Service Provision:

Colfe's School provides excellent network access, including Wi-Fi. Any access issues should be reported to ITSupport@colfes.com. Parents should be aware that cellular-connected devices can bypass the school's security filters. Social media sites are blocked on school devices at all times. However, any use of social media on personal devices would be subject to our Harmful and Abusive Behaviours policy.

Device Use and Management:

Microsoft Surface Pros: Senior School pupils are expected to use Microsoft Surface Pros. The Mobile Device Management system allows remote distribution of updates, settings, and software. Pupils must sign a usage agreement prior to receiving the device (see link below). Expectations include careful handling and protection of the device, keeping passwords confidential, and using the device for learning enhancement only. Misuse will result in sanctions ranging from detentions to suspensions.

Networked Computers:

Pupils have access to OneDrive for storing academic files and are expected to use this platform responsibly. The use of personal computers on the school LAN is prohibited.

Wireless Devices:

Staff and students can connect up to three mobile devices to the school's wireless network by installing an SSL certificate and entering their school credentials. Guests can be issued timed passes for the 'Colfe's Guest' WLAN.

Printing:

The school uses print management software to monitor printed output. All print jobs should be school-related, with networked printers set to default double-sided printing to promote eco-friendliness.

Expectations for Acceptable Use of ICT:

Cyberbullying: Procedures for preventing and addressing cyberbullying are detailed in a separate policy available on the school website.

Pupils: Pupils must not interfere with others' work or the network, ensure academic integrity, not impersonate others or transmit inappropriate messages, seek permission before installing software or sending messages to large groups, and avoid creating, storing, or sending bullying or abusive content.

Emails: Pupils are required to check emails and Teams at least twice daily and compose communications with courtesy and consideration.

Parents: Parents should obtain school permission before publishing data about pupils or staff, attend e-safety lectures, ensure appropriate technology use beyond the school setting, and consult the school's policy on taking and using images of children.

School Obligations: Staff must act reasonably and responsibly with network use, keep workstations and servers secure, maintain current virus protection, manage wireless access proactively, and read and adhere to the school's Data Protection Policy.

Safe Use of Personal Electronic Equipment:

All users must maintain high security over their internet presence, use secure sites, high privacy settings, strong passwords, and avoid disclosing passwords or accessing inappropriate sites.

ICT in the Classroom:

Senior School students must bring their Microsoft Surface Pros to lessons and use them appropriately, adhering to guidelines on device handling, security, and usage for educational purposes only.

Confidentiality:

School information must be kept confidential and used responsibly, both during and after a pupil's time at the school.

Monitoring:

The school reserves the right to monitor communications and network usage to protect pupils, establish facts, prevent crime, and ensure network efficiency. Random checks on devices may be conducted, and internet usage logs are maintained for inspection. Current filtering and monitoring software include Sophos and Senso.

Concerns captured by our software monitoring system of Surface devices are reported to the school. During term time these captures are reviewed daily (Monday to Friday) by the pastoral team. On non-school days i.e. weekends and school holidays, monitoring continues but will not be reviewed until the next school day.

Access:

Students can access the internet via the school's web filter. Mobile phones and other devices are prohibited during the school day except during breaks in designated areas (6th Form only). All other year groups are prohibited from using mobile devices while on the school site.

Inspection of Machines:

The school may inspect pupils' devices if illicit activities are suspected, with inappropriate material being removed and appropriate sanctions applied. Where an indecent image of a child is suspected the device will be seized and stored securely until it can be inspected by a Safer Schools Officer.

Education and Online Safety:

The school aims to educate pupils on responsible online behaviour through classroom teaching, the PSHEE programme, and information evenings for parents. Issues of online safety are regularly addressed to build resilience and awareness.

Working with Parents:

The use of social networking sites can be a particular concern for parents and the School alike. Posting material online about staff or the school without permission is taken seriously and can result in suspension or other sanctions. The school works with parents to promote e-safety, providing specialist advice and encouraging communication about online behaviour. Particular focus is given to advice about the potential hazards and practical steps parents can take to minimise potential dangers. Communications should be used to reinforce the importance of children being safe online, and parents and carers are likely to find it helpful to understand what systems the school use to filter and monitor online use. The school always contacts parents if there are worries about a pupil's behaviour and encourages parents to share concerns with the school.

Please note: an explanation of how and when the school monitors online content can be found in the section 'Monitoring' above.

Mobile Phones and Wearable Technology Usage Guidelines:

Junior school students are not allowed mobile phones or wearable technology.

Year 7 to 11 pupils must have phones switched off during the day and be kept out of sight at all times.

Sixth form students can use phones within designated sixth form areas.

Phones that are misused will be confiscated and held at reception for the remainder of the school day.

Phones must not be used inappropriately, including harassment or theft.

Phones and wearable technology are banned from exam rooms.

Staff are expected to set the example regarding use of mobile phones and social media.

Personal number sharing should not happen; if a member of staff finds their number has been shared, they should alert the DSL. Staff are aware of the dangers of forming relationships via social media or mobile phones, which are outlined in the Staff Handbook and during Child Protection training, and should not hold images of students on personal devices. Further information is available in the school's Acceptable Use Policy for staff.

Reporting:

Technical issues should be reported to itsupport@colfes.com. Breaches of the ICT Code of Conduct should be reported to esafety@colfs.com.

Sanctions:

Breaches of this policy may result in sanctions ranging from device confiscation to exclusion, and criminal activities will involve the Police and Safeguarding authorities. The DSL handles child protection issues.

Additional Policies and Resources:

This policy should be read alongside other school policies and government guidance on safeguarding and online safety.

- [Pupil digital device code of conduct](#)
- [Harmful and Abusive Behaviours](#)
- [Complaints](#)
- [IT Acceptable Use Policy](#)
- [Data Protection](#)
- [Child Protection/Safe Guarding](#)

Updated August 2025

Updated December 2025