



Staff Member Responsible:	NEL
Date Written/Issue Number:	September 2010/v10
Policy Review Date:	March 2026
Date of Circulation to Staff/Consultation (if applicable):	June 2026
Approved by Governors:	30.06.26
Date of Next Review:	March 2027
Required on Website:	Yes

The Gilbert School

Electronic Communications Acceptable Use Policy for Visitors

This policy has been produced in consultation with the Essex County Council Code of Conduct Policy for Schools and Academies. This policy applies to all visitors, guests, contractors, and external individuals who are granted access to the school's Wi-Fi network

This policy should be read alongside other policies of the school, particularly:

- Data Protection Policy
- Safeguarding guide for visitors

This policy outlines the standards and expectations for all visitors using the school's electronic communication systems, network, devices, and internet services. It aims to keep pupils, staff, data, and school systems safe from misuse and applies to all visitors, including contractors, parents/carers, volunteers, governors, and any external professionals accessing school ICT systems or using personal devices on school premises.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Internet

I understand that:

- All use of the school's internet is recorded and the logs uploaded to the school system. Your usage may be monitored to ensure adherence to policies and the law.
- Certain websites or services may be restricted
- The internet should not be used for revealing or publicising proprietary or confidential information.
- Any posting on the internet that causes damage to the school, any of its employees, students or any third party's reputation may amount to misconduct or gross misconduct which could result in dismissal.
- I must not place inappropriate images/video on the internet in any forum and must ensure that background detail (e.g. house number, street name, school) cannot identify me.
- There is no access to social networking platforms under any circumstances.

I understand that I may use the school Wi-Fi for lawful and appropriate purposes only, including:

- Accessing information relevant to their visit or work at the school
- Communication related to educational, professional, or administrative activities
- Limited personal use, provided it is reasonable and does not interfere with network performance

I understand that access to the Wi-Fi network is provided at the school's discretion and may be time-limited or restricted. Access may be withdrawn at any time without notice if misuse is suspected.

I will:

- Take all reasonable measures to ensure that pupils are not exposed to any inappropriate images or web links. This includes remaining in the room when students are using the internet and regularly checking screens.
- Report any accidental access to material which might be considered unacceptable immediately to my line manager and the network manager and ensure it is recorded.

I will not:

- Use the school's equipment, internet or e-mail service for unlawful activities, commercial purposes or for personal financial gain. This includes accessing, downloading, storing, creating, copying or distributing offensive material (including but not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).
- Communicate with pupils or parents using social networking sites (e.g. Facebook). Even offers of assistance to a pupil with studies via social networking sites leaves an employee vulnerable to allegations.
- Access, download, or distribute inappropriate, offensive, or illegal content
- Engage in activities that violate any applicable laws or regulations
- Attempt to gain unauthorised access to school systems, data, or networks
- Transmit viruses, malware, or any malicious software
- Conduct commercial activities unrelated to the school without permission
- Use peer-to-peer file sharing, illegal streaming, or excessive bandwidth consumption
- Harass, threaten, or harm others online

Protecting data

I understand that:

- I must ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the General Data Protection Regulations 2018. This includes the use of 'Strong' passwords and anti-virus software.
- I must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, personal computer or mobile phone) unless that storage system is encrypted and approved for such use by the school. If I am unsure on the sensitivity of data I will contact my line manager and the network manager for clarification.

I will:

- Ensure any devices I use are secure and up to date
- Protect my own personal data and login credentials
- Report immediately any accidental loss of confidential information so that appropriate action can be taken.
- Fully log off, or lock the screen before leaving my laptop or computer unattended.
- Delete or shred any personal or sensitive information that has served its purpose.

I will not:

- Allow a pupil to have individual use of a staff account under any circumstances, for any length of time, even if supervised.
- Store sensitive information in public folders.

School equipment (including iPads and laptops)

I will:

- Protect the school network from damage by ensuring that all memory devices are virus protected and that I do not open e-mail attachments or download files from the internet that I am unsure of.
- Only download apps and other material necessary for work at the school.
- Take all reasonable steps to ensure the safety and security of the equipment. This includes not leaving it unattended and using the protective case provided.
- Make efforts not to intentionally waste resources. Examples of resource wastage include:
 - Excessive downloading of material from the Internet;
 - Excessive storage of unnecessary files on the network storage areas;
 - Use of computer printers to produce class sets of materials, instead of using photocopiers.

I will not:

- Use my own equipment to connect to the school's network unless specifically permitted to do so.
- Use my personal mobile phone or other electronic equipment to photograph or video pupils unless authorised to do so by the member of staff responsible for the visit.

Compliance

By accessing the school Wi-Fi, I agree to comply with this Acceptable Use Policy. Failure to comply may result in immediate termination of access, reporting of illegal activity to relevant authorities and further action where appropriate.

Further advice on all E-Safety issues can be found at; www.ceop.gov.uk, www.thinkuknow.co.uk, www.childnet.com/kia, www.teachtoday.eu. All the teaching and local government union web-sites contain useful advice on communicating safely electronically. **This policy and additional detail can be viewed on the staff X: drive in the 'Policies' folder.** Please report any technical problems immediately to IThelpdesk@gilberd.com or ring 157.

By selecting 'Yes' on the voting buttons on the e-mail accompanying this policy you are agreeing that:

- I understand that by not following these rules I may be subject to legal proceedings and the use of the school's Disciplinary Procedure. Sanctions will depend upon the gravity of misuse and could result in dismissal.
- I confirm that I have read and understood The Gilberd School's **Electronic Communications Acceptable Use Policy for Visitors**.