



Holmer Green Senior School

Acceptable Use Policy

Computer, Communication and
Internet Systems

June 2026

Background and Definitions

Information and communication technologies (ICT), including the internet, cloud services and online communication platforms, are central to education and daily school operations. Holmer Green Senior School is committed to ensuring that students and staff are able to use ICT safely, responsibly and effectively.

The school provides ICT systems and services primarily to support teaching, learning, safeguarding, communication and administration. All users of school ICT systems are expected to use these systems responsibly, lawfully and in accordance with this policy.

This policy defines acceptable and unacceptable use of the school's ICT facilities, systems, devices and network services. It applies to all users including staff, students, governors, contractors, volunteers and authorised visitors.

Use of school ICT systems is subject to UK legislation, including but not limited to:

- UK GDPR and the Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Communications Act 2003
- Keeping Children Safe in Education (KCSIE)
- Prevent Duty guidance

Any illegal or inappropriate use may result in disciplinary action, withdrawal of access privileges, referral to external agencies and/or criminal proceedings.

Acceptable Use

The school provides staff and students with access to:

- School network services
- Internet access
- Email services
- Cloud platforms and online learning systems
- Desktop and portable computing devices
- Printing and storage facilities
- Wireless and BYOD (Bring Your Own Device) services

Use of these services is permitted where it supports educational, administrative or school business purposes.

Users are expected to:

- Use school systems safely, responsibly and professionally
- Respect the privacy and work of other users
- Keep passwords secure and confidential
- Report safeguarding or security concerns immediately
- Comply with staff guidance and ICT procedures
- Take reasonable care of school equipment

The school reserves the right to access, monitor, review and retrieve any data stored on school systems where necessary for safeguarding, security, operational or legal reasons.

The school cannot guarantee that data stored on school systems will never be lost or corrupted. Users are responsible for ensuring important work is saved appropriately.

Users must recognise that inappropriate use of school ICT systems, email or online communication may damage the reputation of the school, even where personal devices or accounts are used.

Staff are responsible for ensuring that materials, websites, videos, presentations and online content used with students are appropriate and suitable for educational use.

BYOD and Wireless Access

The school provides BYOD wireless access for authorised staff, students, governors and visitors.

Use of the wireless network is subject to this policy and any additional WiFi terms presented during connection.

Users must:

- Connect only authorised devices
- Ensure devices are secured with passwords or PINs
- Keep operating systems and antivirus software up to date where applicable

The school's wireless networks are protected but no wireless system can guarantee complete privacy or security.

Monitoring and Filtering

Use of school systems, networks, internet access and email may be monitored for safeguarding, security, network management and legal compliance purposes.

Monitoring will be carried out in accordance with relevant legislation and school policies.

Internet access is filtered and monitored to reduce the likelihood of users accessing harmful or inappropriate material. However, no filtering solution can guarantee complete protection.

Users must immediately report any accidental access to inappropriate content to a member of staff or the ICT team.

The use of unauthorised encryption technologies, anonymising tools or methods intended to bypass school filtering, monitoring or safeguarding systems is prohibited.

Unacceptable Use

The Holmer Green Senior School ICT systems, devices or services must not be used for any of the following:

1. The creation, viewing, storage or transmission of offensive, violent, discriminatory, extremist, obscene or indecent material.
2. The creation or transmission of material intended to cause harassment, distress, intimidation, inconvenience or anxiety.
3. The creation or transmission of defamatory, abusive or threatening communications.
4. Accessing, creating or distributing pornography, adult material or content promoting sexism, racism, homophobia, religious intolerance, violence or hatred.
5. Accessing or distributing material encouraging illegal activity, radicalisation, extremism, terrorism or substance misuse.
6. Using social networking, messaging or streaming platforms outside authorised educational use.
7. Downloading, copying or distributing copyrighted material without permission.
8. Storing or transmitting material likely to damage the reputation of the school or members of the school community.
9. Sending unsolicited commercial messages, spam or advertising.
10. Attempting unauthorised access to systems, accounts, files, services or devices.
11. Accessing, changing, deleting or using another user's files, data or credentials without explicit authorisation.
12. Sharing passwords or allowing another person to use a school account.
13. Using personal email accounts for official school business.
14. Installing, downloading or running unauthorised software or applications.
15. Introducing malware, viruses, spyware or other harmful software.
16. Deliberately disrupting systems, networks or the work of others.
17. Excessive personal use of storage, bandwidth or ICT resources.

18. Playing, downloading or distributing games or non-educational media without permission.

19. Connecting unauthorised hardware or peripherals to school systems without approval from the ICT Support team.

20. Attempting to disguise identity, impersonate another user, forge email headers or bypass network controls.

21. Using proxy services, anonymising software, VPN services, encrypted tunnels or any other method intended to bypass the school's filtering, monitoring or safeguarding systems.

22. Connecting personal VPN applications, browser VPN extensions or external remote-access services to school devices or networks without explicit written approval from the ICT Manager.

23. Using artificial intelligence (AI) tools in a way that breaches examination regulations, copyright, data protection requirements or academic integrity expectations.

24. Recording, photographing or sharing images, video or audio of staff or students without appropriate permission.

Additional Policies for Staff

Staff must use school ICT systems professionally and in accordance with safeguarding, GDPR and confidentiality requirements.

Staff must:

- Lock computers when unattended
- Protect confidential information from unauthorised viewing
- Ensure printed documents containing sensitive information are secured
- Use only approved systems and applications for school business
- Carry out routine housekeeping of files and storage areas
- Remove former students from online learning platforms promptly where appropriate
- Report lost or stolen devices immediately to the ICT Manager
- Ensure portable storage devices containing personal or confidential data are encrypted
- Encrypt emails containing sensitive, confidential or GDPR-related information when sent externally
- Follow all published ICT security, safeguarding and data protection procedures

Staff must not:

- Access school systems from insecure public computers or internet cafés
- Use school systems for unlawful or inappropriate personal activity
- Display unverified online content to students
- Circumvent school security, filtering or monitoring systems

All software, media and digital resources used within school must be used legally and in accordance with licensing requirements.

Data Protection and Security

All users must comply with the school's data protection and information security requirements.

Personal data must:

- Only be accessed where necessary
- Be processed securely and lawfully
- Not be shared inappropriately
- Be stored only on approved systems and locations

Users must immediately report:

- Suspected data breaches
- Phishing emails
- Security incidents
- Loss of devices containing school data
- Accidental disclosure of confidential information

Safeguarding and Online Safety

All users are expected to contribute to a safe online environment.

Any safeguarding concern involving ICT or online activity must be reported immediately in line with the school's safeguarding procedures.

This includes:

- Exposure to harmful content
- Online bullying or harassment
- Grooming concerns
- Extremist content
- Suspicious communications
- Inappropriate image sharing

Compliance and Sanctions

Users accessing third-party systems or services through the school network must comply with the acceptable use requirements of those systems.

Failure to comply with this policy may result in:

1. Temporary suspension of ICT access
2. Permanent withdrawal of ICT access
3. Internal disciplinary action
4. Safeguarding intervention
5. Referral to external agencies or law enforcement where appropriate

Serious breaches may result in immediate suspension of access pending investigation.

The school reserves the right to investigate any suspected misuse of ICT systems.

Review

This policy will be reviewed annually or sooner where required by changes to legislation, safeguarding guidance or technology.

Reviewed: June 2026

Next Review: June 2027