Holmer Green Senior School

Acceptable Use Policy Computer, Communication and Internet Systems

February 2022

Holmer Green Senior School

Acceptable Use Policy
Computer, Communication and Internet Systems – February 2022

Background and Definitions
Information and communication technologies (ICT) such as the internet are radically changing the world in which we live and work. Schools have an important role to educate and train people in the proper use of them. Holmer Green Senior School is committed to bringing the maximum benefits of ICT possible to its students and staff, and to equipping them with the knowledge, skills and attitudes that will enable them to thrive in the digital age

This policy defines acceptable and unacceptable use of the school's ICT facilities. Users are expected to adhere to this Policy at all times. Appropriate use of the systems promotes efficient use of the systems and allows equipment to be available in good order at all times. The use of school computing resources and facilities are subject to UK law and any illegal use will be dealt with appropriately.

Acceptable Use

The school provides each student and staff member with access to the school network, access to the internet, use of an IT device and an email account. The use of these resources is permitted and encouraged by the school where it is suitable for academic and teaching purposes and supports the goals and objectives of the school. The internet must be used in accordance with the school's standards of conduct and to support educational related activities.

The school reserves the right to open any data or files stored in any form on the network. Staff and students are responsible for their own backups in respect of data or files that are important to them. The school takes no responsibility for any data loss or for damage to any media, such as USB sticks, used on school machines.

Users must be aware that inappropriate use of the internet and any electronic communication, such as email, from school equipment can potentially damage the school's reputation, whether or not a school email address is used in the communication. Staff should recognize that the use of a school email address in an electronic communication, and the fact that the correspondent is a school employee, implies a degree of official status. Staff must check, as far as possible, that materials, presentations, websites or media that they show or print for students, or ask students to view, do not contain any offensive or objectionable items, adverts, pictures or links to such.

The school also provide Bring-Your-Own-Device "BYOD" WiFi access for staff, students, governors and official visitors to the school. Its use is also governed by this policy and the BYOD WiFi network terms that staff and students have to 'Accept' every time the wireless is used.

Use of the network, WiFi, internet or intranet and email, including data sent on it, may be subject to monitoring for security and network management reasons. Monitoring will be in line with the statutory RIPA (Regulation of Investigatory Powers Act) legislation. The school site is also recorded by CCTV and these recordings may be kept on archive recordings and used or processed in line with the appropriate legislation and the school's CCTV policy.

The schools' internet provision is filtered and every effort is made to prevent inappropriate content being accessible. All users are reminded that, in order to ensure compliance with this Policy, *all* School systems are monitored and *all* emails may be recorded or intercepted (in line with appropriate legislation) and that the use of proprietary encryption technologies is not permitted.

Unacceptable Use

The Holmer Green Senior School ICT systems or equipment may not be used for any of the following:
1 The creation, viewing or transmission of any offensive, violent, degrading, discriminatory, obscene or indecent images, text, data or other material, or any data capable of being resolved into obscene or indecent images or material.
2 The creation, viewing or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.

3 The creation or transmission of defamatory communications, for example, insulting, derogatory or slanderous email.
4 The creation, viewing or transmission of offensive materials, for example, adult materials, images or pornography, or materials including 'jokes' that show or promote sexism, racism, religious intolerance, homophobia or violence or in any other way contravenes the school's Equal Opportunities Policy.
5 The creation, viewing or transmission of materials that encourage or either endorse the financial exploitation of a crime or that encourage the use of illegal substances.
6 The creation, viewing or transmission of materials that are either ideologically radical or extremist related.
7 The use or access of social networks/media, unless as part of a supervised and authorised classroom activity
8 The transmission or storage of material that infringes the copyright of another person or organisation. Students and staff making use of ICT facilities must respect copyright and not plagiarise the work of others by working in accordance with the appropriate copyright legislation. This also includes the storage of third-party copyright materials such as MP3 files or videos.
9 The transmission or storage of material, whether intended for public consumption or not, which might be construed through the nature of its content to reflect negatively on the reputation of the school or on individuals or groups of individuals at the school.
10 The transmission of unsolicited commercial materials or advertising.
11 Deliberate unauthorised access to facilities or services accessible via school network.
12 To examine, change, or use another person's files or data for which they do not have explicit authorisation.
13 The sharing, theft, use or misuse of another user's, or email, logon details including usernames and passwords, with or without that users' permission.
14 The use of personal e-mail accounts to carry out school activities is forbidden. All school related activities must be done using an official school e-mail account and the same e-mail account must be used when signing up for online services as a school participant.
15 Deliberate activities with any of the following characteristics:
- Corrupting or destroying other users' data
- Violating the privacy of other users
- Disrupting the work of other users, including any action or activity that reduces the class or study time available for others
- Using any amounts of storage space on the school's e-mail or network systems for personal materials
- Continuing to use an item of software or hardware after it has been requested that use cease because it is causing disruption to network systems.
- Other misuse of the school network or networked resources, such as the introduction of viruses, malware or spyware
- Disguising, attempting to disguise or forging identity or usage when sending email, using network facilities or browsing the internet; this includes, for example, the use of proxy bypass or the use of anonymous or forged email.
- Misusing the identity of the school in a financial or business transaction over the internet to imply the official status of the purchaser
- Using school network facilities for the playing, downloading, installing or distribution of games, web games, or materials, software or media which is copyrighted by a third party
- Attaching items of equipment or peripherals that do not belong to the school to the school's computers, networks or systems without explicit authorisation from the IT Support Services team (for example, MP3 players, digital cameras, PDAs). The one exception to this are USB memory sticks, which are acceptable as long as they are not used to copy software installed on school networks or to copy school copyright information for personal use (NB: school systems are protected by anti-virus software).

Additional Policies for staff

Staff not are allowed to use school systems for personal or recreational use. Staff should also carry out routine housekeeping of files and resources they have stored on school systems. This includes the removal of obsolete resources, videos and files. Additionally, staff that use online learning platforms should ensure that the records or files of students who have left the school are promptly removed from

any online classes they have created (with the exception of maintaining records for possible exam moderation). These classes must only allow log-in of students who are currently enrolled in the school.

- Staff should ensure that confidential information is not visible to others, including ensuring that any computer screen is not overlooked and that any printouts are not left unattended
- Staff should "Lock" their computer screens when away from their terminal.
- A number of internet, e-mail or ICT related activities are governed by law, or other school policy or published regulations and are therefore clearly unacceptable.
    - These include online stalking, grooming, internet luring, soliciting of children by computer, defamation, retention of offensive screen savers, fraud, software theft, damage to school systems, retention of other people's personal details or information, drug-related activities, or any other illegal activity
    - These will be regarded by the school as constituting misconduct and any staff involved will be subject to disciplinary action up to and including dismissal.
- Webpages, e-mails, videos, audio and materials used by each member of staff are their individual responsibility. Any materials shown or made available to students either electronically, displayed on screen or projector or printout must be checked beforehand by each individual member of staff personally to ensure compliance with these guidelines and statutory obligations. It is the responsibility of staff to therefore check that any web searches, documents, videos, audio, web-links, websites or e-mails that they use or show to students are safe to use and not to rely on any system of web filtering.
- All portable storage devices (such as, but not limited to – USB flash and hard drives) containing any data which is either regarded as i) Confidential ii) Financial in nature or iii) Classed as containing Personal Data (in-line with the appropriate legislation) MUST be encrypted using the school's systems. Personal data can include, but is not limited to, staff and student names, timetables, mark sheets or performance data. A user guide on how to encrypt and password protect USB devices is available.
- Emails concerning financial, sensitive, confidential or GDPR-classed data to recipients outside the school must be sent securely.
- Staff must be familiar with and process personal data in accordance with the GDPR legislation and the HGSS published guidelines.
- Staff that have been issued with a laptop must also comply with the School's Laptop Policy. Laptops designated for staff use must not be lent to students.
- All software, movies, music and resources used within school must be done so legally. School systems prevent the ad-hoc installation of software.
- Copyright movies must only be played or used in school where the school retains a physical 'hard' copy of the movie.
- Staff must immediately report to the ICT Manager/Business Manager the loss of any mobile or computing device (school owned or personal) which has either school data, e-mail or app access installed.

- **<u>Compliance</u>**

It is the responsibility of all users to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of school network does not occur. Where necessary, service may be withdrawn from a user if any conditions of the Policy are violated.

This may take one of two forms:

1 A temporary withdrawal of service of either all or select computer services, usually for a period of about two school weeks. After appropriate warnings have been issued to the student or member of staff concerned, the **Headteacher** will authorise the withdrawal of service and **arrange for the ICT Manager to** notify the students' tutor or member of staff's line manager. Reinstatement of access will be made only when the **Headteacher, ICT Manager** and the student's tutor or member of staff's line manager are satisfied that appropriate steps have been taken to ensure that any unacceptable behaviour does not occur again.
2 An immediate suspension of service, should a serious violation occur, or a violation causing disruption to computer services. Such a suspension would be made on the judgement of the **Headteacher and ICT Manager.** The student's tutor or member of staff's line manager would be notified immediately.

Where violation of these conditions is illegal or unlawful, or results in loss or damage to school network resources or the resources of third parties accessible via the school network, the matter may be

referred for legal or police action. The use of HGSS facilities is subject to UK and EU law and any illegal use will be dealt with appropriately.

Reviewed: February 2022

Next Review: February 2024