HEATHFIELD SCHOOL
IT Acceptable Use Policy

Policy Area:	General
Relevant Statutory Regulations:	ISSR 2014 Part 3 NMS Part B, Standard 4 and Part D, Standard 8 Data Protection Act 2018 Keeping Children Safe in Education 2023
Key Contact Personnel in School	
Nominated Member of Leadership Staff Responsible for the policy:	Manager of IT Network and Services
Version:	2024.01
Date updated:	01 September 2024
Date of next review:	01 September 2025

This policy will be reviewed at least annually, and/or following any concerns and/or updates to national and local guidance or procedures.

Overview

Heathfield School (the "School") is committed to protecting the staff, governors, pupils and visitors who make up the School community from illegal or damaging actions by individuals, either knowingly or unknowingly. The purpose of publishing an Acceptable Use Policy is to ensure the School's established culture of openness, trust and integrity prevails.

Internal and external systems, including but not limited to computer, networking and server equipment, mobile devices, software, operating systems, storage media, network accounts providing email, web browsing or file storage, are the property of the School. These systems are to be used for business purposes in serving the interests of the School.

Effective security is a team effort involving the participation and support of every School community member who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at the School. The rules are in place to protect the community member and the School.

Inappropriate use exposes the School to cyber risks including virus attacks and ransomware, compromise of network systems and services, data breach, and related legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct School business or interact with internal networks and school systems, whether owned or leased by the School, staff, governors, pupils or a third party. All staff, governors, and pupils are responsible for exercising good judgement regarding appropriate use of information, electronic devices, and network resources in accordance with the School's policies and standards. Exceptions to this policy are documented in **5.2**.

This policy applies to all staff, governors, and pupils at the School.

Policy

General Use and Ownership

School information stored on electronic and computing devices whether owned or leased by the School, staff, governor, pupil or third party, remains the sole property of the School. Users must ensure through legal or technical means that information is protected in accordance with the *Data Protection Standard*.

Users have a responsibility to promptly report the theft, loss or unauthorised disclosure of School information.

Users may access, use or share School information only to the extent it is authorised and necessary to fulfil assigned job duties.

School staff and governors are responsible for exercising good judgment regarding the reasonableness of personal use. Use of the Internet for non-education related activities is acceptable provided a balance is maintained and it does not encroach on the needs of work, study, research, or the delivery of lessons.

The use of School systems, such as email, for the purpose of running another business, is strictly prohibited.

For security and network maintenance purposes, authorised individuals within the School may monitor equipment, systems and network traffic at any time.

The School reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Staff or governors are not permitted to enter into any contract or subscription on the Internet on behalf of the School, without specific permission from IT Systems and/or the Bursar.

All documents, applications and email messages which are created or developed at School or on a School computer remain the property of the School. Such documents, applications or messages may not be used at another workplace without specific consent in writing from the Headmistress.

All School devices must be returned, complete with charger and any other supplied accessories, on termination of employment. The cost of replacing any device not returned or returned damaged may be deducted from the staff members final salary payment.

Acceptance of a laptop computer implies agreement in full with this IT Acceptable Use Policy. If a computer is lost, stolen or damaged, the Bursar or Manager of IT Network and Services must be notified in the first instance. The staff user may be charged for the cost of replacement if the device is lost or damaged due to negligence.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network require authentication for access and a security certificate to be installed on the device.

User level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a pin or password protected lock screen. Users must lock the screen or log off when the device is unattended.

Any public page featuring a School member of staff or governor must be kept clean, presentable and must not in any way bring the School into disrepute.

All social network accounts are required to have basic security set to ensure maximum privacy against all non-'friends'.

Users must use caution when opening email attachments received from unknown senders, which may contain malware.

Door security fobs and cards are for the use of the issued user only and should not be loaned to any other person. The loss of a door security fob or card should be reported to IT Systems immediately.

Unacceptable Use

The following activities are, in general, prohibited. School staff, governors, or pupils may be exempted from these restrictions during their legitimate job or school responsibilities (e.g IT Systems staff may have a need to disable the network access of a device if that device is disrupting the network).

Under no circumstances is an employee of the School authorised to engage in any activity that is illegal under English law while utilising School-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with **no** exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the School.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photography from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the School or the end user does not have an active license is strictly prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
- Revealing School network account password/passphrase to others or allowing use of your School network account by others. This includes family and other household members when work is being undertaken at home.
- Making fraudulent offers of products, items or services originating from any School account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties. For the purposes of this section, "disruption"

includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited without prior approval from IT Systems.
- Executing any form of network monitoring which will intercept data not intended for the specific user, unless this activity is a part of the Staff members normal job/duties.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the School network.
- Providing information about, or lists of, the School staff, pupils, clients, visitors or similar to parties outside the School, unless where required to allow third parties to provide a service to the School, such as photographers, local health initiatives or training providers. Data Protection Impact Assessments should be conducted before collecting and transferring such information.
- It is forbidden for anyone to disconnect School devices from power or network ports in order to connect their own unless approved by IT Systems.
- Attempting to circumvent content, firewall or security restrictions put in place by IT Systems, including the use of external proxies or VPNs is expressly prohibited.
- Internet sharing from a 4G or 5G enabled phone, tablet or laptop device (also known as 'personal hotspot', 'Internet sharing' or 'portable hotspot') is strictly forbidden on School premises. Action will be taken when a hotspot is detected.
- Peer2Peer or torrenting software is not permitted on any device connected to the School network.
- Attempting to gain access to the Server Room, IT Office, IT Store or any network cabinet is forbidden.
- Eating or drinking in any computer suite or the Server Room is prohibited.

Email, Communication and Social Media

When using the School resources to access and use the Internet, staff and governors must realise they represent the School. Whenever staff or governors state an affiliation to the School, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the School". Questions may be addressed to IT Systems.

The following are strictly prohibited from any School account or by using the School's network.

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages. Messages must not contain offensive, obscene, threatening or libellous language or be construed as such.
- Bullying messages (cyber bullying) will be treated with the same level of seriousness as physical bullying. The school adopts a zero tolerance approach to any cyber bullying issues; all staff will challenge any abusive behaviour between pupils that comes to their attention and will immediately report the same to the Designated Safeguarding Lead any issues of this nature. Please see the *Child Protection and Safeguarding Children Policy* for further details about dealing with child-on-child abuse.
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the users account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Social networking between staff and pupils is strictly forbidden.

In addition, the following restrictions should be noted:

- No pupil may possess or use a social network account on any device if they are under the age of 13 years. This is a child safeguarding requirement and any breach will result in a mandatory inquiry.
- The use of blogging, social media and or social networking platforms by staff or governors, whether using School devices and systems or personal devices and systems, is also subject to the terms and restrictions set forth in this policy.
- Staff, governors and pupils are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Heathfield School's *Data Protection Standard* when using social media.
- Any public page featuring a member of staff, governor or a pupil must be kept clean, presentable and must not in any way bring the School into disrepute.
- All social network accounts are required to have basic security set to ensure maximum privacy against all 'non-friends'.
- Staff, governors or pupils may not attribute personal statements, opinions or beliefs to the School when using social media.
- It is forbidden to use School logos or any other School intellectual property in connection with any blogging or social media activity unless expressly authorised by IT Systems and/or the School Marketing department.
- Staff should not use personal devices to take photos or videos of pupils. Pupils may not use their personal devices to take photos or videos during lessons, and should ask permission of the subject to take photos or videos at any other time.

Policy Compliance

Compliance Measurement

IT Systems will verify compliance with this policy through various methods, including, but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by IT Systems in advance.

Non-Compliance

Any staff, governor, or Pupil found to have violated this policy may be subject to disciplinary action.

Related Standards, Policies and Processes

- Data Protection Standard
- Password Policy
- Anti-Bullying Policy
- Record Keeping Policy
- Child Protection and Safeguarding Children Policy