Hinchingbrooke School

Hard Work High Standards Kindness

Policy Statement
on

INFORMATION AND COMMUNICATION TECHNOLOGY ACCEPTABLE USE FOR STAFF AND GOVERNORS (AUP)

Revised:	3 Yearly
Date approved by Governing Body:	October 2023

STAFF GUIDELINES

At Hinchingbrooke School students and staff work together to create a mutually respectful and purposeful learning environment. The school expects staff, students and all who have access to the IT systems (including governors), to take a responsible attitude in all matters. As a professional organisation with responsibility for students' safeguarding it is important that everyone with access to the school systems take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

The Computer system and all components are the property of Hinchingbrooke School and are provided as a resource to be shared by all who are given access. Computer facilities, including mobile units, are made available to further student education and for staff to enhance their professional activities, including teaching, research, administration and management. The school's Acceptable IT Use Policy has been drawn up to protect all parties. A full copy of the school's Acceptable IT use policy is available on the school's intranet and all users click to accept this when they log in to the system.

Please be aware that the below policy guidelines are not exhaustive and staff and governors are expected to use the network and IT facilities in a professionally responsible manner that is in keeping with other school policies and the law.

To ensure that members of staff and governors are fully aware of their professional responsibilities when using Information Technology and the School systems, they are asked to read and sign this Acceptable IT Use Policy.

A. The School Network and Digital Security

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, email and social media sites.
2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate the commission of further offences, or to modify computer material without authorisation.
3. I understand that any hardware and software provided by the School for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I understand that the equipment provided by the School is for use by School employees and that I am responsible for looking after the equipment.
4. I will respect system security and I will not disclose any password or security information to anyone. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 6 or more characters and is only used on one system).
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the IT Technical Team.
6. I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act 1988 and that my practice complies with the requirements of GDPR. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
7. I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted.
8. I understand that Copyright and Intellectual Property Rights must be respected.

9. I will report all incidents of concern regarding student's online safety to the **Designated Lead Child Protection Officer** (Tony Heath) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator. I have read and understood the ***e-Safety and Acceptable Use*** from the **current Safeguarding and Child Protection Policy**[2].
10. I understand that no data belonging to the school or any personal data relating to students should be stored on any device without being authorised and encrypted by the network manager. (Note: data stored in the cloud is automatically encrypted.)
11. I understand that it is a criminal offence to use any school IT equipment or networks made available by the school for a purpose not permitted by the school. All network and Internet use must be appropriate to education and staff professional activity. Irresponsible use may result in the loss of network or Internet access.
12. I understand that use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted or anything likely to bring the school into disrepute.
13. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the IT Technicians as soon as possible.
14. I am aware that network access or access to mobile devices must be made only via the user's authorised account and password, which must not be given to any other person. I have read and understood the **Bring Your Own Device (BYOD) Policy**[1] documentation.
15. I have read and understood the School's policy relating to use of students images and agree to adhere to these guidelines.

Policies on e-Safety and acceptable use, set out in a separate document, are reviewed regularly by the governing body. They reflect the balance needed between the exciting opportunities offered by the internet and other technologies and the need for students and staff to keep themselves safe and deal sensibly with risk.

B. Email Communications

1. As a user, I am responsible for all e-mail sent and for contacts made that may result in emails being received.
2. I will ensure that all messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers or be published on social media. I will ensure that appropriate *'netiquette'* will be applied.
3. I am aware that email activity that threatens the integrity of the School ICT systems, or activity that attacks or corrupts other systems, is forbidden.
4. As a user, I must take care not to reveal personal or sensitive information through email, personal publishing, blogs, messaging or removable storage devices.

C. Mobile Phone Communication and Instant Messaging

1. Staff are advised not to give their home telephone number or their mobile phone number to students. Mobile phone communication should be used sparingly and only when deemed necessary. A school device should be used in the event of excursions taking students off site as managed by the EVC.
2. Photographs and videos of students should not be taken with mobile phones unless for official purposes such as tweeting golden antlers' winners or hot choc Friday students
3. Staff are advised not to make use of students' mobile phone numbers either to make or receive phone calls or to send to or receive from students' text messages other than for approved school business.
4. Staff should only communicate electronically with students from school accounts on approved school business.
5. Staff should not enter into instant messaging communications with students.

D. Social Networking

The school recognises the educational potential of Web 2.0 Technologies including and not limited to Social Networking, Blogging, Micro Blogging and media sharing sites.

The school encourages staff to use these technologies for research purposes and the sharing of good practice. In using such technologies and platforms staff should adhere to the following guide taken from **"Keeping Children Safe in Education" (DfE)**. Staff should:

1. Not mention the school in a negative manner. This includes all stakeholders (students, colleagues, parents).
2. Refrain from commenting on incidents that occur within the school directly.
3. Ensure that personal social networking sites are set at private and that students are never listed as approved contacts.
4. Not give their personal contact details to students, including their mobile telephone number.
5. Only use equipment e.g. mobile phones, provided by school/service to communicate with students~~,~~ making sure that parents have given permission for this form of communication to be used.
6. Only make contact with students for professional reasons.
7. Recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible.
8. Not use internet or web-based communication channels to send personal messages to a student.

In General

Communication between students and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a student. They should not request, or respond to, any personal information from the student, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. Staff should never have students as friends on social networking sites such as Facebook.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. Use of mobile devices while not connected to the school network will be monitored by Sophos or similar software once reconnected.

This documentation can be accessed on the Staff Intranet under '*General Policies'* or by contacting the HR department.

Reference to other documentation held within these policy guidelines:

[1] Bring Your Own Device (BYOD) Policy

[2] Safeguarding and Child Protection Policy

Hinchingbrooke School

Hard Work High Standards Kindness

ICT Acceptable Use Policy for Staff

Staff User Agreement

Please read through this policy documentation carefully and return a signed copy of this page to the HR department.

I hereby consent to adhere to Hinchingbrooke School's '*Acceptable IT Use Policy*' outlined in this document. I understand that I am responsible for the reporting of any misuse of this policy relating to school network systems, hardware devices or software programmes.

Staff/Governor Name: _____

Staff/Governor Signature: _____

Job Title: _____

Date: _____

For Office use only

Date received:

Added to file: