REVIEWED: AUTUMN 2023
NEXT REVIEW DATE: AUTUMN 2024
REVIEWED BY: HEAD OF OPERATIONS
RATIFIED BY: COMPLIANCE COMMITTEE

SPIRITU INSPIRATUS
Hazelwood School

Acceptable Use of ICT, Mobile Phones and other Electronic Devices Policy

This Policy includes the Early Years Foundation Stage

Introduction

Hazelwood School aims to ensure secure access to ICT for all pupils. This policy outlines the acceptable use of internet and electronic communication facilities, fileservers, messaging services, and any networks or hardware, including but not limited to that provided by the School. It applies to any personal devices and other equipment that can be used to access, store or record data or media files.

The School recognises that social media encourages a new collaborative way of thinking and exploring information with considerable ease. It is important that pupils, parents and staff are able to identify and verify material found on the web for its own worth: they should not be so naïve as to think that information is immune from being inappropriate, biased, bullying or exploitative in nature. It is not enough to impose a list of restrictions; Hazelwood School wishes to educate and safeguard pupils, parents and staff on the best use of ICT and alert them to the dangers and recognises that the community is no longer bound by the physical campus.

This Policy establishes acceptable and appropriate use of Hazelwood School and Hazelwood Nursery and Early Years (collectively known as ‘the School’) technology and protect both users and the School. It should enable the School to safeguard and promote the welfare of pupils and staff and to minimise the risk of harm to the assets and reputation of the School. It should also serve to prevent abuse of email and internet facilities.

This must be read with consideration to the General Data Protection Regulation (GDPR) and the School’s Data Protection Policy and may be subject to change from time to time. Questions relating to GDPR should be submitted to the Head of Operations.

It is the users' responsibility to ensure that they comply with this Policy at any given time, and this policy may be revised, without notice, at any time. Logging onto the School systems is deemed to be an agreement to this Policy.

All staff are responsible for seeing that School ICT is used in an effective, ethical and lawful manner and with consideration to others.

The School provides technology for educational and administrative applications for its pupils and staff. In general, School ICT may be used in connection with core teaching, administration, and research work. Certain non-core users that do not consume resources or interfere with other users are also acceptable. Under no circumstances may staff use School

ICT in ways that are illegal or that will threaten the School's reputation or charitable status, or that interfere with reasonable use by other members of the School Community.

Staff are responsible for the well-being of the children in their care and must ensure children are not accessing or communicating with extremist groups. Children who the staff feel are showing worrying interests in extremist, abusive or other inappropriate content should be raised immediately with the Designated Safeguarding Lead.

School ICT is deemed to be:

- any hardware, software or data (including web/cloud based) owned by the School or present on the School site;
- any data brought into the School environment from elsewhere; and
- any School data held online or in offsite storage or hardware taken offsite.

Users may not store large amounts of personal data on the Schools ICT, including but not. exclusively photos. Any photographs, particularly those of pupils, that are taken should be. downloaded or deleted as soon as possible. Staff should ensure their device is logged with the Head of Operations on the Photographic Devices Log.

If a member of staff reaches the limit of their My Documents quota with work files, they can ask for this to be increased. If a user uses on-line/cloud storage it is their responsibility to make sure it conforms to GDPR and is backed up.

As Network Administrator, the School reserves the right to monitor any or all network, internet, and email traffic at any time and for whatever reason, at its sole discretion, without notice or notification as deemed appropriate. All users agree to such monitoring by their use of the School's ICT.

Use of School or personal hardware
The School has a number of approved devices which can be borrowed when the need arises.

Data controlled by GDPR should only be taken off site on secure, encrypted laptops or USB memory devices that are provided by the School.

If you take any School hardware offsite you must take reasonable care of it. It should be stored in a secure location and if left in a car it should be out of sight in a locked boot. No School hardware should be left unattended on public transport. Any personal data leaving the site should be encrypted on a laptop or memory device provided by the School. School ICT is for the use of staff and pupils only and must not be used by other family members.

It is the responsibility of the user to back up any data created on local devices as a protection against theft or hardware or software malfunction. Any School ICT loaned to staff will be returned upon the staff member leaving the School and remains at all times the property of the School. All School laptops are encrypted as well as password protected.

Usernames, passwords and system security
Usernames and passwords are confidential. Staff must not disclose their password nor permit pupils to work using a member of staff's login details. Users must log off or lock their pc, or other device, when left unattended to ensure the security of the system. The ICT Department must be notified immediately if a user's password is compromised. A password change will be enforced every 90 days. If requested, Staff may be issued with a password for the wireless network. This is for the connection of School mobile devices only. Other personal devices are not permitted to connect to the wireless network unless under very special circumstances.

Should a user access the School's data, including the user's email, from a personal computer, tablet or handheld device, that is outside the control of the School, the user is responsible for taking reasonable precautions to protect the data. The device must have the latest operating system and anti-virus/malware, password protection and if possible, encryption. Should the device be lost or stolen the ICT Department should be informed so the user's password can be changed. Setup, security and troubleshooting of personal devices is the responsibility of the user. No personal devices are to be connected to the School's main wired or School wireless networks. Personal devices include, but is not limited to, laptops, iPads, mobile phones and wearable technology such as smart watches, where the device could connect to the internet. Wearable technology that connects directly to the internet without touching the School networks should still not be used to access School data, including email.

Use of the internet and of email

The School's email systems are available for communicating matters directly related to the School.

Although it is accepted that some personal emails may be exchanged during the working day these should be kept to a minimum and should not impact on their employment and should not reflect badly on the School. Users may not view, send, or retrieve inappropriate files. Care should be taken in the opening of emails. Emails from unknown sources, or those that are unexpected, should be deleted without opening. From time to time, training will be made available to staff on this, and other matters. Staff should make time to complete any such training.

The content of emails should be consistent with the standards of other written communication. Emails should not include defamation or falsehood, sending or distributing of gossip or messages maligning a person, a group of persons or an organisation (including the School), unlawful harassment and/or discrimination on any grounds 'electronic bullying' between staff and/or pupils or use of any other content which would be detrimental to the School's reputation.

Use of the internet will be strictly controlled and monitored. Users take responsibility for using the internet in a safe manner and not for illegal or inappropriate activities.

Staff should check all websites before accessing them in a class and should check that the whole page, including adverts, is appropriate. Some of the images and text available on them may be harmful or offensive to pupils, staff, and the School Community as a whole. In the case of blocked sites, staff can send the ICT Department the URL of the site to be added to the staff or all users allowed lists only once they have checked at home that the site is safe.

If you receive an email that you suspect to be a scam such as spam, an attempt to obtain personal information or attachments that may spread malicious code please contact the ICT Department immediately.

Use of Google Classroom

When using Google Classroom, the School's virtual learning environment, the rules that apply to other access of the School's data also apply. In addition users accept that links to web based educational resources may result in links to onward sites being available, for example YouTube links, and whilst care should be taken by staff to ensure that sites are appropriate for the user, they cannot be responsible for all onward links. Internet filtering takes place on the School site but when accessing the internet, including Google Classroom, from outside School users accept that there may be some risks associated with using the internet.

Use of social media

The School reserves the right to block sites including social media as it deems appropriate. It is against School policy and safeguarding regulations for any member of staff to make friends with or accept a friend request from any pupil who is currently studying at the School. It is against School policy and safeguarding regulations for any member of staff to make friends with or accept a friend request from any pupil or former pupil under the age of 18. No reference should be made on personal blogs or social networking sites to the School, or its employees, that are derogatory, defamatory, discriminatory, or offensive in any way or which could bring the School into disrepute. The contents of blogs and social network sites can be used by the courts in cases of litigation as well as a reference to interviews or future career decisions.

Conditions of use

Anyone using School ICT does so at their own risk. The School and its employees cannot be held responsible for any equipment damage or data loss or corruption that may be suffered as a result of using School ICT including but not exclusively in the event of hardware, or software, failure or virus outbreak.

Misuse of computers is a serious disciplinary offence. Misuse includes but is not limited to: fraud, theft, system sabotage, attempted hacking or unauthorised access, introduction of viruses, installing, or attempting to install, software, breaches of GDPR, sending or forwarding inappropriate emails, compromising your own, or others', passwords, share or distribute material protected by copyright without obtaining the permission of the owner, use of School ICT for illegal purposes, phishing or dissemination of spam email including chain letters. Any attempt to use School ICT to threaten, intimidate or bully staff, pupils or other persons is prohibited.

Users may not download, install, or store software unless it is part of their job requirement. Where a member of staff makes a serious breach of the AUP, the Governors have authorised the Head or Head of Operations to, if appropriate, apply the School's Disciplinary Procedure which may lead to dismissal.

The School's liability in respect this Policy is limited as follows:

- Unless negligent under the terms of this Policy, the School accepts no responsibility to the pupil, parents or staff caused by, or arising out of, a pupil's or member of staff's use of email and the internet whilst at School.
- Access to the network and internet may be affected by interruptions out of the School's control or necessary technology maintenance.

Taking, Storing and Using Images of Children

We are an open and inclusive community that is very proud of all of the achievements of all of our pupils in their academic, artistic and sporting endeavours. We celebrate both success and participation by the taking of photographs and videos which we like to share with parents, pupils and prospective families through newsletters (The Nutshell), on-line, in local advertising and within school marketing material (e.g. Our Prospectus).

Parents who accept a place for their child at Hazelwood are provided with Terms and Conditions which detail the use of images. By signing the Acceptance of a Place Form, parents are granting the School permission to use images of their child(ren). If parents wish to withhold this permission, they are required to provide a separate, and written, request/statement.

Any changes to the information given by the child's parents should be sent in writing and acknowledged by the School.

Full details of the School's Data Protection Policy are available on request.

Pupils like to be photographed and to see their work displayed so we hope that parents will feel able to support the School by consenting to the School using images in the ways described herewith.

Periodically, the School will request updated preferences for the use of images, detailing the different locations and uses including making a distinction between individual and group shots. Once this information is collated, this database will form the most recent and therefore applicable source of permissions for image usage.

Security

All photographs of children are kept in a discreet area of the School server (Marketing Photos) which is accessible only to limited members of staff or within the staff server, which requires a login and password to gain access. Any parent who requests an image will be sent a copy subject to time and considerations of appropriateness.

Children will be accompanied by a member of staff when photographed by a professional photographer. Parents are given the opportunity to purchase copies of any photographs taken for promotional purposes by professional photographers and class and sports teams photographs. A link to a secure on-site gallery will be provided from which to make their choice. The password to access the gallery will only be given to the parents of the relevant team, cohort, or group of children. Selection and payment transaction will be directly with the photographer or host of the on-line Gallery. Payment will ensure families only purchase those few photos which are personal to them and avoids a mass-download situation which would be contrary to prevailing safeguard protocols.

The images that the School uses for displays and communication purposes will not identify an individual pupil by their full name. Pupils will be identified by their first name, or the group, team name or event they are associated with. The School only uses images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc in their proper context alongside a report of the event or to promote the curriculum of that year's group or department.

Storage and Review

The School will backup photographs on a regular basis.

Nominated school cameras and other photographic appliances.

We will only take images of pupils on School equipment and all these images will be downloaded onto the secure server, which can only be accessed by staff.

Staff will not use personal devices to take photos or videos unless these devices are on the Schools registered list of acceptable equipment. This list is updated termly.

Parents are permitted to take photographs of their own children taking part in sporting and other school events. They should attempt to minimise the numbers of other children captured in the image.

The School welcomes images and recordings from parents and all such media will be used within the guidelines set out in this Policy.

Parents should use their cameras and recording equipment with consideration and, when appropriate, are reminded by the School that they should not post images and recordings onto the internet or social media without the consent of parents of children recorded.

Early Years Foundation Stage Mobile Phone and Camera Policy

To ensure the safety and welfare of the children in our care there are specific protocols for the use of personal mobile phones and cameras in the early years and nursery setting.

- No personal mobile phones, cameras and video recorders can be used on the Hazelwood Nursery and Early Years (HNEY) site when in the presence of children either on premises or when on outings.
- All staff mobile phones must be turned off and placed in the designated locked cupboard either in the room or relevant office. Phones may only be checked at break times in the staff room and never in the rooms, or in the toilets. All phones must be signed in and out of the designated areas.
- No parent, visitor or member of staff from the Hazelwood School site (HSS) are permitted to use their camera, mobile phone or use the mobile's camera facility on the HNEY site in the presence of children.
- School policy regarding the use of mobile phones and cameras will be clearly communicated to parents at the information evening and at all events. All rooms display signs reminding staff, parents and visitors that mobile phones are not permitted.
- In the case of a personal emergency, staff should use the School telephone. It is the responsibility of all staff to make families aware of the School telephone numbers.
- Personal calls may be made in non-contact time but not within the teaching areas or toilet facilities.
- Personal mobiles, cameras or video recorders should not be used to record classroom activities. ONLY School equipment as registered on the central Nominated Devices listing such as cameras and iPads should be used. Photographs will only be taken provided the necessary photographic consents are in place.
- Photographs and recordings can only be transferred to and stored on a School computer before printing.
- All telephone contact with parents/carers must be made on the School telephone.
- During group outings nominated staff will have access to the School mobile which can be used in an emergency or for contact purposes.
- In the case of productions and special events, parents/carers are permitted to take photographs of their own child in accordance with School protocols which strongly advise against the publication of any such photographs on social networking sites. Where possible, the performance will be recorded on a school device and shared with parents.

The use of iPads in school

iPads are used throughout the School. Pupils in Years 6-8 have an individual device for them to use at both School and at home. There are pods of iPads which will be available for teachers to use throughout the other year groups.

Staff with ipads have signed a separate AUP governing their use. Pupils are given a list of do's and don'ts which they, and their parents, are required to sign governing safe use of the device. Furthermore, spot checks of pupils' devices and their use are carried out to ensure compliance and appropriate sanction taken if required. Devices are only used when supervised by staff. The taking of photographs, unless for a class or topic-related project, is not allowed. Any breach of these conditions will result in action being taken against the pupil(s) involved.

Ratified by Compliance Committee on 24 November 2023