Hazelwood School

PUPIL ICT ACCEPTABLE USE POLICY - YEAR 3 TO YEAR 8

Introduction

The ICT Acceptable Use Policy (AUP) is designed to establish acceptable and appropriate use of Hazelwood School (the School) technology and protect both users and the School. It should be signed by parents on behalf of themselves and their children.

The School provides technology for pupils to use in lessons and to support their learning. Under no circumstances may pupils use School ICT in ways that are illegal or that will threaten the School's reputation, or that interfere with reasonable use by others. School ICT includes any hardware, software or data owned by the School, and any information or data created, edited or viewed on School hardware or created in School and accessed away from School.

Aims

This Policy aims to encourage pupils to make good use of the growing educational opportunities presented by access to the internet and the use of email and other electronic media whilst promoting the welfare of pupils and minimising the risk of harm to the assets and reputation of the School.

This Policy must be read with consideration to the General Data Protection Regulation (GDPR) and may be subject to change from time to time. Questions relating to the GDPR should be submitted to the Data Protection Officer. Further details can be found by reading the School's Privacy Notices. All can be found on the School website.

By signing the Terms and Conditions, parents are agreeing to the aims of this policy, and will make their child aware of the contents of this policy. Logging onto the School systems is deemed to be an agreement to this AUP.

This AUP may be revised, without notice, at any time. Parents will be contacted for major changes only.

If you have any queries or do not agree with this policy, please contact Head of Operations.

Objectives

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

Pupils should understand that they should not disclose to anyone their usernames and passwords other than their parents, teacher, or the Senior IT Technician/Data Manager. Their teacher may keep a record in the event that pupils forget their password. If pupils have their password changed for any reason it is their responsibility to tell their parents of the change. Pupils should only log on as themselves. When leaving a pc, or other device, pupils must log off to allow other pupils access to the machine. If you think another pupil, or person outside of the School, knows your password, then please contact the Senior IT Technician/Data Manager who will change your password for security reasons.

Hazelwood School

No personal devices should be brought into School as these are not protected or filtered and therefore present security and child protection risks. If a need is identified i.e. for learning support, the School will consider purchasing a device to meet the needs of the pupil.

Pupils should look after the data they store in their My Documents folder and Google Drive. They should not store large numbers of photos or pictures or non-school related files and should delete old work when told to by their teachers. Learning to manage data is a very important lesson and ensures that pupils do not reach the limit imposed on their My Documents folder. Any pupil reaching the limit may contact the Senior IT Technician/Data Manager regarding additional space if needed.

Use of the Internet will be strictly controlled and monitored and many filtering rules are in place which are tiered by age range to block inappropriate, offensive and radical content amongst others. However, when a pupil uses the internet, they take responsibility to use the internet in a safe manner including not deliberately seeking content which may breach the School policies. Many filter rules are set by the websites themselves e.g. Google Images and "safe" images and certain web pages may still contain images, and/or text, that is contrary to individual parental beliefs and thoughts as to what is appropriate. Whilst every attempt is made by the School to provide a safe internet experience, no filtering solution is perfect.

The use of USB storage devices is restricted and only School approved devices can be used. Any unapproved devices connected to the School network will be automatically rejected by the system and reported to the Senior IT Technician/Data Manager.

When using Google Classroom, the rules that apply to other access of the School's data also apply. When using Google Classroom 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 will be taken by staff to ensure that sites are appropriate for the pupils 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. Pupils must not abuse the inbuilt messaging facility.

When using School ICT neither the School nor its employees can be held responsible for any equipment damage or data loss or corruption.

Misuse of computers is very serious. Misuse includes, but is not limited to: fraud, theft, attempted hacking or unauthorised access, introduction of viruses, installing, or attempting to install, software, sending or forwarding inappropriate emails including chain letters, compromising your password, sharing or distributing material protected by copyright without obtaining the permission of the owner, use of School ICT for illegal purposes. Any attempt to use School ICT to threaten, intimidate or bully staff, pupils or other persons is not allowed.

Google mail accounts should be used sensibly. For example, pupils may not view or send inappropriate files, including lies or unkind comments about staff or other pupils (electronic bullying) or to involve themselves with extremist or anti-social groups. The content of emails should be consistent with the standards of other written work and will be filtered on a key word search. There may be other examples that have not been listed. Care should be taken in the opening of emails. Emails from people you do not know, or are not expected, should be treated very carefully and if in doubt delete without opening. In the event of opening an email the child finds upsetting they should raise concern with their parents or staff. A copy of the School's Online Safety Policy covering this area is available as part of the overall

Hazelwood School

Safeguarding Policy.

Pupils may not download, install or store software on School Hardware except in the case of the School issuing 1:1 mobile devices when separate rules will apply. In this case a separate policy will be signed when the device is issued.

Where a pupil is found not to have followed the Policy this will be dealt with by the relevant teacher, Head of Year or the Head, depending on the seriousness of the situatioN.

Approved by SMT in November 2024

REVIEWED: AUTUMN 2024
NEXT REVIEW DATE: AUTUMN 2025 REVIEWED BY: HEAD OF OPERATIONS RATIFIED BY: HEAD (IN CONSULTATION WITH SMT)

Hazelwood School