HIGHDOWN SCHOOL AND SIXTH FORM CENTRE

ICT AND INTERNET RESPONSIBLE USE POLICY

Aspiration – Respect – Excellence

Monitoring, Evaluation and Review

Author	Mr M A Grantham Head of School	Review Period	3 years
Version	1	Status	Approved
Committee	Learning and Teaching Committee	Date Approved	October 2023
Link Governor	Dr C Foulkes	Review Date	October 2026

HIGHDOWN SCHOOL AND SIXTH FORM CENTRE
ICT AND INTERNET RESPONSIBLE USE POLICY

This policy should be read in conjunction with the following policies:

- Online Safety Policy
- BYoD Policy
- Safeguarding and Child Protection Policy
- Prevent Policy
- Behaviour Policy
- Anti-bullying and Discrimination Policy

Introduction

This policy outlines an acceptable code of conduct for the use of the ICT equipment and systems within our school.

The school provides computers and networked resources for student use in teaching classrooms and other resource areas. As part of this facility, Internet, e-mail and school-owned software are available for use on the proviso that these resources are used for the purpose of education.

It is the school policy to respect all computer software copyrights and adhere to the terms and conditions of any licence to which Highdown School is a party.

Responsible use

- The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. This includes indecent images, extremist or discriminatory material, racial or religious hatred. If you are unsure, or if you come across anything which makes you feel uncomfortable, you should turn your computer monitor off and let a teacher know.
- Every student has a different computer login and password. Passwords must conform to the school's password protocol. They should never allow anyone else to use their details. Students must change your password if they think someone else may have their details. They should seek assistance with this from the Network Team.
- Students must never share any personal information online.
- Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people. Students must not access any websites or social network pages that promote such views. The school has systems in place to block extremist material and monitor students who try to access it. Any student found accessing such material will be reported to the relevant authorities.
- Students should never try to bypass any security in place, including using proxy bypass sites. The security is in place to protect users from illegal sites, and to prevent hacking into other people's accounts.
- Students must not attempt to access other people's files or accounts.

- Students should never take information from the internet and use it as their own. This is plagiarism. A lot of information is copyright, which means that somebody else owns it and it is illegal to use this information without permission from the owner. If unsure, students should ask an adult.
- Students should be respectful online, and not behave in an abusive manner. They should consider what they are saying, and how somebody else might read it. All emails are traceable to the school and emails sent from an email account are the responsibility of the individual account holder.
- Students should not attempt to access/use social networking sites, chat rooms, or gaming sites, nor should they attempt to access any inappropriate, offensive or illegal content. Filtering and monitoring systems are in place across the school network.
- Students should not use their school email to subscribe to mailing lists.
- Mobile phones must be turned off and kept inside school bags during the school day. The only exception is when a teacher requires students to use their device as part of a lesson. Students must never take photographs or film themselves, friends or others without permission. Students should not forward inappropriate images/videos they have received from somebody else. They should tell an adult immediately if they have received illegal, inappropriate or offensive content.
- The internet, or other ICT communication media, must not be used to bully, harass or discrimintate against others. It can have very serious consequences. Students should report incidents of cyber-bullying to an adult in school or Safeguarding Team.
- Everyone should treat school ICT equipment with care and respect. They must not deliberately damage or vandalise ICT equipment. They must report any problems to a member of staff. Students are responsible and accountable for a device they may be loaning for the day at school, including any damage caused.
- During any asynchronous or synchronous lessons, via Microsoft Teams, students must follow the principles of this policy. Furthermore, they must keep cameras turned off for synchronous lessons, and must not record or take screenshots from the lesson. Microphones will be set to mute and controlled by the class teachers. Chat functionality will also be managed and monitored by the class teacher. Students misusing this function will be removed from the lesson.
- Students should only use Microsoft OneDrive for sharing files between devices and not USB/Flash drives.
- Students must not seek to share or download large files which may slow internet speeds for other users.
- Student accounts will be deleted when students leave the school. It is their responsibility to save any files in another location before leaving.
- Students must ensure they log-off the network, websites (e.g. Class Charts), etc. when they have finished using school ICT equipment.
- BYoD is used in school for the purposes of education and should only be used in lessons, when directed to do so or agreed by the class teacher. Use of BYoD is subject to this Responsible Use Policy.

Failure to follow this guidance, or deliberate misuse of School ICT, may result in a sanction, in accordance with the Behaviour Policy.

The school assumes you students have read and understood all of the above and that they understand that any of their electronic communications could be looked at, and they they understand that any electronic communications related to school are not entirely private.

Monitoring, evaluation and review

The Network Manager and Senior Leader responsible for Whole-school ICT will monitor the effectiveness of this policy, in liaison with Heads of Achievement and the Safeguarding Team.