Scarborough College

ICT ACCEPTABLE USE POLICY

This is a whole College policy, including EYFS and the boarding community, all staff, pupils, parents, contractors and visitors

1.0 Policy Scope

This policy outlines what are acceptable and unacceptable uses of ICT facilities within Scarborough College (non-exhaustive examples shown in the appendix).

1.1 Staff, Parents & Visitors

Access to college systems is not intended to confer any status of employment or contract. In this policy 'staff' includes teaching and non-teaching staff, governors and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers or contractors. Whilst we aim to support the full use of the vast educational potential of new technologies we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect pupils, staff and visitors from e-safety incidents and promote a safe e-learning environment for pupils.

1.2 Pupils

At Scarborough College we believe that pupils should be trusted to use digital technologies in a principled and productive way. This policy gives everyone the opportunity to make productive decisions in the ways they choose to use digital technologies. Scarborough College has a responsibility to provide safeguards against risk, unacceptable material and activities.

- Policy ethos: *We should all be fully engaged in the ongoing debate about what responsible digital citizenship means and how this can be nurtured and developed within the school.*

2.0 Technology Behaviours

As a member of the College community you are expected to follow these principles in all of your online activities:

2.1 The college cannot guarantee the confidentiality of content created, shared and exchanged via the college systems. Ensure that your online communications, and any content you share online are respectful of others, composed in a way you would wish to stand by and do not detriment the reputation of Scarborough College.

2.2 Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination or extremism, or raises safeguarding issues).

2.3 Respect the privacy of others. Do not share photos, videos, contact details or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.

2.4 Do not access or share material that infringes copyright, and do not claim the work of others as your own.

2.5 Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

2.6 Staff must not use their personal email or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

3.0 Use of ICT Systems

Whenever you use the College's IT systems (including connection of your own device to the guest Wi-Fi network) you should follow these principles:

3.1 Only access College IT systems using your own username and password supplied by Scarborough College IT Services (SCITS). Do not share your username or password with anyone else.

3.2 Do not attempt to circumvent the content filters or other security measures installed on the College's IT systems, and do not attempt to access parts of the system that you do not have permission to access.

3.3 Do not attempt to install software on, or otherwise alter, Scarborough College IT systems.

3.4 Do not use the College's IT systems in a way that breaches the principles of online behaviour set out above.

3.5 Be aware that Scarborough College monitors use of IT systems and the College can view content accessed or communicated via its systems.

3.6 Virus protection software must not be tampered with or its messages ignored. Warnings, Messages or Errors must be reported to SCITS immediately.

3.7 Any person accessing Scarborough College IT systems must have read and signed to agree with this policy before being issued with login details to the Scarborough College network; including, either with a corporate issued device or a "bring your own device (BYOD)" connecting to the guest network.

4.0 Login Details/Passwords

It is the College's policy and practice that all staff and pupils who have access to any IT Resources are responsible for choosing passwords and protecting their login information. All Scarborough College login information, IT resources and data must have adequate password protection. The policy covers all users who are responsible for one or more accounts or have access to any resource that requires a password. Passwords protect the College's network and computer system, are your responsibility and should **NOT** be shared with anyone else.

4.1 Passwords should be unique and memorable and must meet the following standards:

- Be at least eight characters and contain a combination of upper/lower case letters, numbers and at least 1 special character (if the IT system allows). These requirements will be enforced with software when possible but all users should apply this guidance to keep data safe. In addition, all users should use common sense when choosing passwords by avoiding basic combinations e.g. "password", "password1", 123456, birthdays, family names etc.

- Staff and pupils must not use the same passwords for their college accounts as they do for their personal accounts or devices. Passwords should be changed monthly and where currently possible, will be enforced by software.

Neither staff nor pupils can use password managers or other tools to help store and remember passwords without express permission from SCITS. All users should be mindful of phishing scams and external attempts by criminal individuals or organizations to obtain/steal passwords and access data. Applying these practices will help prevent this and further guidance can be sought from SCITS.

5.0 Data Protection.

If you think your login credentials have been compromised or you suspect that your login details or data are at risk, please contact the SCITS team immediately at:

- mark.smith@scarboroughcollege.co.uk Tel: 01723 344209 (x209)
- brandon.castleton@scarboroughcollege.co.uk Tel: 01723 344701 (x701)

5.1 All known breaches of data or risk to Scarborough College GDPR practices, will be reported to the Data Protection Officer immediately, in line with the Data Protection Act 2018.

NOTE: Ensure that your IT devices are locked/logged-out when you leave them unattended and that any sensitive information is not viewable by anyone else whilst you are using your device.

6.0 SCITS Property

All IT equipment issued specifically to you will be recorded on the SCITS asset management database and a copy kept on your personnel/pupil file. It is your responsibility to look after this equipment and take reasonable steps to protect it from theft, loss or damage. You will be liable for the costs of repair or replacement should you fail to take reasonable care (except for normal wear and tear). On leaving the College you must return all items issued to you. The College also provides access to computers for all staff in the common room, classrooms and departmental bases. Please report all faults or breakages without delay to the SCITS team.

7.0 Use of College Systems

The provision of College email accounts, Wi-Fi and internet access is for official College business, administration and education. Staff and pupils should keep their personal IT requirements separate from their college IT use.

7.1 Please be aware of the College's right to monitor and access web history and email use. Any inappropriate or unapproved use of the internet or the college network is strictly forbidden and may result in disciplinary action being taken. Online shopping is not permitted (except with prior authorisation when access is required for educational resources), nor access to any illegal sites, gambling, 'adult' sites or fraudulent activity. The College has restrictions in place to limit access to such sites. As new websites, apps etc. appear daily, 3rd party monitoring software may not yet be updated, in which event, should these fail and inappropriate material is available to view, you must report this to the SCITS team immediately.

7.2 Staff must be aware that email communication can form (or amend) a legally binding contract and therefore must ensure that they do not commit or imply commitment to any contractual arrangements without authorisation. The email system is monitored and staff should not expect privacy in email communications sent using this account or from College equipment. The deletion of emails from inboxes or archives does not mean that they cannot be recovered for the purposes of disclosure.

7.3 Trivial messages and jokes should not be sent or forwarded through the email system. Not only could this cause distress to recipients (if inappropriate) but could also cause the College's IT system to suffer delays or damage. All work related documents should be saved in either Google Docs or the College's internal drives. Confidential documentation should be password protected and, if relevant, your line manager must be informed of the password.

8.0 Use of Personal Devices or Accounts and Working Remotely

All official College business of staff and official educational use by students, must be conducted on College systems, and it is not permissible to use personal email accounts for College business or official educational use by students. Any use of personal devices for College purposes, and any removal of personal data or confidential information from College systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be for College related activities[1]. Documents containing confidential information or personal data should not be stored on mobile devices or accessed remotely, unless express permission from the Head has been sought.

8.1 Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the College's policies. Such devices must be password/pin protected and where applicable software accessed must be logged off when not in use. The password/pin should be changed regularly and not shared with anyone. The College reserves the rights to request to check that the device and therefore its contents, are secure and Staff will be obliged to surrender the device for this reason. Where a member of staff leaves employment, the College also reserves the right to request and have access to any personal device used in relation to work to ensure that all data, access to systems and College apps have been deleted. If deletion has not occurred the College will undertake the deletion. In case of the Headmaster, Deputy Head and the Business Manager their College accounts and mobile devices will be set up with a 'kill switch'.

8.2 The SCITS team are working longer–term on a "Bring Your Own Device" (BYOD) system to enable future increased functionality and security for those wishing to use their own devices. This policy will be updated in line with this development once rolled out to the Scarborough College community.

9.0 Monitoring and Access

Scarborough College uses **ESET Endpoint Security** for antivirus purposes, **DUO Two Stage Authentication** software for secure login procedure and **Smoothwall/Go Guardian** online monitoring software applicable to both staff and students.

9.1 Staff, parents, pupils and all visitors should be aware that College email and internet usage (including through College Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and College email accounts may be accessed by the College where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

9.2 Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The College may require staff to conduct searches of their personal accounts or devices if they were used for College business in contravention of this policy and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

10.0 Compliance with Related School Policies

You will ensure that you comply with the College's Data Protection Policy.

11.0 Social Networking Sites

All use of social media and the internet on College equipment/networks is monitored and any misuse in relation to social media which is brought to the College's attention, will be investigated and may result in disciplinary action.

11.1 Whilst the College is unable to control the personal accounts of staff, pupils or parents, you are reminded that your actions may reflect on the College and any action which may bring the College into disrepute will be investigated and may result in action being taken. All staff are advised to ensure their privacy settings are set accordingly. It would be considered inappropriate to have pupils as friends on any social media network on a personal account. Depending on the circumstances, it may also be inappropriate to have parents as friends.

11.2 You must be mindful of how you present yourself and the College, on both the internet and any social media accounts. The wider life of staff or anyone affiliated to Scarborough College can have professional consequences and this must be considered at all times when sharing personal information. When posting/communicating online you should consider whether the contents would be more appropriate in a private message. While you may have strict privacy controls in place, information could still be shared by others. It is always sensible to consider that any information posted may not remain private.

11.3 Under no circumstances must you divulge or comment on any information gained in the course of your work or study, or relating to any groups or individuals the College provides a service to, on any social media outlet. Any views expressed should be your own and this should be clear. You should not post anything that may offend, insult or humiliate others. You must not post anything that could be interpreted as threatening, intimidating or abusive. You must not post disparaging or derogatory remarks about the College or its governors, staff, volunteers, pupils or parents/families.

11.4 The College acknowledges that pupils and staff members may wish to set up personal web forums or blogs. This should be done outside of College hours and not using College equipment. No association to the College should be made without prior permission of the Head. Staff are reminded to consider the content of such websites and blogs to ensure no conflict in relation to their role in the College.

11.5 Any breach of this policy will be investigated and may result in action being taken. The College's own social media accounts are updated only by authorised personnel.

12.0 Resident Boarding Staff

Staff living in the boarding houses may use the College network and equipment to access the internet for their own personal use during non-working hours. While such use is permitted, you must not do anything which may bring the College into disrepute or contravene the terms of this policy.

13.0 Shared Drives, Data Storage and Data Retention

All work related documents should be saved in either Google Docs or the College's internal drives. Confidential documentation should be password protected and your line manager must be informed of the password. Confidential email communications must be sent using appropriate software such as Egress. Staff should avoid storing any confidential or personal information (such as pupils' details) on portable drives/USB sticks. Where it is necessary, the data should be password protected and be deleted from the device at the earliest opportunity.

13.1 Any old portable drives/USB sticks should be destroyed by the IT department, who will ensure all data is removed. SCITS are intending to use encrypted data methods moving forward, this policy will be updated once in use.

13.2 Staff and pupils must be aware that all emails sent or received on College systems will be routinely deleted or where applicable archived. In addition, email accounts will be suspended immediately or closed and the contents deleted within one year of that person leaving the College. Important information that is necessary to retain will be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with College policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the College's email deletion protocol.

13.3 If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Business Manager. Staff should also refer to the College's Data Protection Policy and associated documents.

14.0 IT Waste Disposal of Equipment and Storage Media

Staff, students and visitors should avoid storing any confidential or personal information on portable drives/USB sticks. Where it is necessary, the data should be password protected, encrypted and deleted from the device at the earliest opportunity. All IT waste, including any old portable devices/USB sticks, should be disposed of by SCITS in line with their IT/Electronic Waste Disposal Policy.

15.0 Data Breach Reporting

The law requires the College to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

15.1 This will include almost any loss of, or compromise to, personal data held by the College regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the College's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal

15.2 The College must generally report personal data breaches to the ICO without undue delay, i.e. within 72 hours, and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the College must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

NOTE: If either staff or pupils become aware of a suspected breach, please notify the Business Manager immediately.

15.3 Data breaches will happen to all organisations, but the College must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The College's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

16.0 Breaches of this Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the College's usual procedures. In addition, a deliberate breach may result in the College restricting your access to College IT systems. If you become aware of a breach of this policy, or you are concerned that a member of the College community is being harassed or harmed online, you should report it to the Business Manager and Deputy Head. Reports will be treated in confidence.

ELECTRONIC ACCEPTANCE OF THIS POLICY

Please confirm that you understand and accept this policy by sending a response back to the person who sent you this e-mail **and type the following in to the reply e-mail;**

"I have read and agree to the Scarborough College IT Acceptable Usage Policy"

This will be retained for Scarborough College's records and act as proof of your policy acceptance.

OR

DIGITAL ACCEPTANCE OF THIS POLICY

You may use a digital signature if you have access to a digital pen.

If you are able to digitally sign, please e-mail the digitally signed copy of this form to hr@scarboroughcollege.co.uk (Staff) or tim.cashell@scarboroughcollege.co.uk (Students).

I understand and accept this IT Acceptable Use policy.

Name (please print): .....

Signature: ..... Date: .....

Policy Prepared by:

Mark Smith
IT Coordinator
v1.02

Person Responsible for Updates	Date Last Reviewed	Next Review Due
Alison Higgins	January 2023	December 2023

Appendix

Examples of acceptable use are (These lists are not exhaustive):

- Using web browsers to obtain information from the Internet.
- Accessing databases for information as needed.
- Using e-mail for contacts.
- Using the school's network to promote the exchange of information to further education and research and is consistent with the mission of the school.
- Using the school's network to access outside resources that conform to this 'Acceptable Use Policy'.
- Using the network and Internet in a manner which respects the rights and property of others.
- Keeping all accounts and passwords confidential and inaccessible to others.
- Showing responsibility by making backup copies of material critical to you.
- Showing responsibility by taking precautions to prevent viruses on the school's equipment.
- Upon receipt of an attachment, checking to make sure it is from a known source.
- Backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use, and notifying a teacher, supervising adult or your manager of the occurrence immediately.
- Logging out or locking computers when they are left unattended.
- Recognising that electronic communications sent through or stored on the school's network will be treated as school related and may be monitored or examined by the Headmaster or his authorised delegates for operational, maintenance, compliance, auditing, security and/or investigative purposes.
- Reporting any damage to or loss of computer hardware immediately.
- Saving documents onto appropriate storage areas of the school network or other appropriate storage systems.
- Reporting any inappropriate behaviour and online bullying to the relevant person.
- Taking reasonable care that there is no damage or loss of any equipment on loan from school.

Examples of unacceptable use are (These lists are not exhaustive):

- Creating, accessing or forwarding illegal, offensive, inappropriate, unethical, harmful to the school, or is non-productive/non work related.
- Creating, sending or forwarding chain e-mail, i.e. messages containing instructions to forward the message to others.
- Recording, filming or taking photographs on school premises without permission
- Broadcasting e-mail, i.e., sending the same message to more than ten recipients or more than one distribution list.
- Relocating school information and communication equipment without prior permission.
- Conducting a personal business using school resources.
- Transmitting any content that is illegal, offensive, harassing or fraudulent.
- Using inappropriate language: do not swear, use vulgarities or sexual innuendos.
- Creating, sending or forwarding material likely to be offensive, inappropriate or unacceptable to recipients.
- Using programs that harass school users or infiltrate a computing system and/or damage the software components is prohibited.
- Changing original software setting/configuration of school owned computers.
- Doing harm to other people or their work.
- Installing software on school computers unless authorised by the ICT Team.
- Doing damage to the computer or the network in any way, or failure to take reasonable care of data accessed.
- Interfering with the operation of the network by installing illegal software, shareware or freeware.
- Plagiarism and violation of copyright laws or other intellectual property right.
- Conversation in e-mail using all upper case letters. This is considered shouting.
- Sharing your passwords with another person. Doing so could compromise the security of your files.
- Wasting limited resources such as disk space or printing capacity.
- Trespassing in another's folders, work or files.
- Removing software CDs from their rightful location
- Giving out personal information such as your home address or telephone number.
- Downloading material from the Internet without specific authorisation from the ICT teacher or Network Manager.
- Viewing, sending or displaying offensive messages or pictures.
- Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts of terrorism, harassment, murder, suicide or other illegal activity.
- Unauthorised use of the College's facilities for personal use.
- Posting confidential information regarding the College, its staff, pupils or their families at any time.