IT POLICY

TRINITY CHURCH OF ENGLAND HIGH SCHOOL	**Reviewed by:**	Governors' Curriculum Committee
	Approved by:	Full Governing Body
	Date approved:	9th July, 2019
	Next review due by:	End of 2021/22 academic year

Contents

AIM/PURPOSE

The aim of this policy is to ensure that all users of IT associated with Trinity are clear about its intended use. IT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of IT within our society as a whole. Currently the internet technologies students are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter, Instagram and SnapChat
- Mobile/Smart phones with text, video and~~/or~~ web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

GENERAL PRINCIPLES

At Trinity Church of England High School, we understand the responsibility to educate our students on eSafety Issues; teaching them the appropriate behaviour and critical thinking skills to enable them to remain safe and within the law when using the internet and related technologies, in and beyond the classroom.

All schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress. Poor management of sensitive information can result in media coverage, damage to the reputation of the school and potentially a fine. Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling must be aware of the risks and threats and how to minimise them. This can make it more difficult for the school to use technology to benefit learners.

Both this policy and the Staff and Student Acceptable Use Policies are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, visualisers, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

STANDALONE STAFF AND STUDENT IT ACCEPTABLE USE POLICY AT TRINITY CHURCH OF ENGLAND HIGH SCHOOL

The Governors have adopted Acceptable Use Policies for staff and students, these provide simple and straight forward statements that staff and students are required to indicate their agreement to.

Monitoring of Acceptable Use policies

Authorised IT staff may, with good cause, inspect any IT equipment owned or leased by the school at any time without prior notice.

Authorised IT staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving staff, students, visitors, ITT students or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school IT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulations, or to prevent or detect crime.

Authorised IT staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any school related issues retained on that account.

Breaches of Acceptable Use policies

A breach or suspected breach of policy by staff, students, visitors, ITT students or contractors may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual.

For staff, any policy breach is grounds for disciplinary action in accordance with the school disciplinary procedure. Policy breaches may also lead to criminal or civil proceedings.

For students, breaches will be dealt with in accord with the school’s behaviour policy.

The school is subject to GDPR regulations for information please see Data Protection Policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school’s relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are: Deputy Head (Curriculum), IT Manager and Business Leader.

Systems and Access

- Teachers and Pastoral tutors are issued with a laptop computer for the duration of their employment at the school to enable them to undertake their duties. This laptop remains the property of the school, any damage or loss should be promptly reported to the IT Manager. It is the responsibility of the individual to return the laptop, and any other school IT equipment in their possession at the end of their employment with the school to the IT Manager.

- Users are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school IT equipment or their own device.

- Users must not allow any unauthorised person to use school IT facilities and services that have been provided to them.

- Users must ensure they remove portable media from their computer when it is left unattended.

- Users must only use their own personal logons, account IDs and passwords and do not allow them to be used by anyone else.

- Staff are to keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information.

- Staff must ensure they lock their screen before moving away from their computer during a normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

- Users are to logoff from the PC completely when they are going to be away from the computer for a longer period of time.

- Users must not introduce or propagate viruses.

- It is imperative that users do not access, load, store, post or send from school IT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.

- Where necessary, staff should obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

- It is essential that any hard drives which may have held personal or confidential data are ‘scrubbed’ in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever is appointed to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides students with supervised access to Internet resources (where reasonable) through the school’s fixed and mobile internet connectivity.

- Staff will preview any recommended sites, online services, software and apps before use.

- Searching for images through open search engines is discouraged when working with students.

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

- All users must observe copyright of materials from electronic resources.

Internet Use

- All users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

- Do not reveal names of students or any other confidential information acquired through your job on any personal social networking site or other online application.

- The school’s Twitter and other social media channels are to be used in accordance with the training provided to nominated staff.

- On-line gambling or gaming is not allowed.

It is at the Head’s discretion as to what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Our school employs web-filtering which is the responsibility of the IT Manager.

- Staff and students are aware that school based email and internet activity can be monitored and explored further if required.

- The school does not allow students access to internet logs.

- The school uses management control tools for controlling and monitoring workstations.

- If staff or students discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the IT Manager or teacher as appropriate.

- It is the responsibility of the school, by delegation to the IT Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the IT Manager's to install or maintain virus protection on personal systems.

- Students and staff are not permitted to download insecure resources, programs or files on school based technologies without seeking prior permission from the IT Manager.

- If there are any issues related to viruses or anti-virus software, the IT Manager should be informed.

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. The school endeavours to deny access to social networking and online games websites to students within school.

- Staff may only create blogs, wikis or other online areas in order to communicate with students using the school's virtual learning platform or other systems approved by the Head.

- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored.

Email

All staff should have a personal email address that forms part of the staff record. This is to enable notices regarding pensions, emergency school closure, etc. to be communicated independent of the school email system.

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits, including direct written contact between schools on different projects, be they staff based or student based, within school, nationally or internationally. We recognise that students need to understand how to style an e-mail in relation to their age and how to behave responsible online.

Managing e-mail

- The school gives staff their own e-mail account to use for all school business as a work based tool**.** This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- Staff should use their school email for professional communication.

- It is the responsibility of each account holder to keep their password secure.

- For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for school business.

- Under no circumstances should staff contact students, parents or conduct any school business using their personal e-mail addresses

- All e-mails should be written and checked carefully before sending in the same way as a letter written on school headed paper.

- Staff sending e-mails to external organisations, parents or students are advised to cc. the Head, line manager or designated line manager.

- Students may only use school approved accounts on the school system and only for educational purposes.

- E-mails created or received as part of a member of staff's job will be subject to disclosure in response to a request for information under the Freedom of Information Act. Staff must therefore actively manage their e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- All student e-mail users are expected to adhere to the accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Students must immediately tell a teacher / trusted adult if they receive an offensive or upsetting e-mail.

- Staff must inform the eSafety co-ordinator or line manager if they receive an offensive e-mail.

- Students are introduced to e-mail as part of the first module of Enquiry Skills.

- However users access their school e-mail, whether directly, through webmail when away from the office or on non-school hardware all the school e-mail policies apply.

Sending e-mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Security Section.

- Users are to use their own school e-mail account so that they are clearly identified as the originator of a message.

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

- School e-mail is not to be used for personal advertising.

Receiving e-mails

- Check your e-mail regularly.

- Activate your ‘out-of-office’ notification when away for extended periods.

- Never open attachments from an untrusted source; consult the System manager first.

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

- The automatic forwarding and deletion of e-mails is not allowed.

Mobile Technologies

Emerging mobile technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. It is not recommended that a member of staff contact a student or parent / carer using their personal device.

- This technology may be used for educational purposes, as mutually agreed with the Head. The device user, in this instance, must always ask the prior permission of the bill payer.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices (including iPads and phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Users must never interfere with any anti-virus software installed on school IT equipment.

- If a machine is not routinely connected to the school network, provision for regular virus updates must be made through the IT team.

- If a user suspects there may be a virus on any school IT equipment, they are to stop using the equipment and contact the school IT Manager.

Data Security

- The school gives relevant staff access to its Management Information System, with a unique username and password.

- It is the responsibility of everyone to keep passwords secure.

- Staff are aware of their responsibility when accessing school data.

- Staff have been issued with the relevant guidance documents and the Policy for IT Acceptable Use.

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.

- Staff should avoid leaving any portable or mobile IT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked and out of sight.

- Staff should carry portable and mobile IT equipment or removable media as hand luggage, and keep it under your control at all times.

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared multi-function printers are used.

- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent.

Disposal of Redundant IT Equipment

- All redundant IT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- All redundant IT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any ~~ICT~~ IT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations

  Data Protection Act
  Electricity at Work Regulations

- The school will maintain an inventory of all its IT equipment including a record of disposal

- Any redundant IT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

eSafety

eSafety - Roles and Responsibilities

eSafety is seen as an aspect of Safeguarding at Trinity High School, given the complexity of the issues involved whilst a lead is taken by the school Designated Person for Safeguarding, the Head of IT, Computing and Enquiry Skills and the Deputy Head (Curriculum) share a responsibility for eSafety. As a team they should keep abreast of current issues and guidance.

The school invests annually in the eSafe monitoring system which through a combination of automated protocols and human assessment reports worrying behaviour from IT users in school.

eSafety in the Curriculum

IT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills and eSafety in Enquiry Skills lessons

- Educating students about the online risks that they may encounter outside school is also done informally when opportunities arise

- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are

- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals

- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online

- Students are asked to report any incidents of Cyberbullying to the school

- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent / carer, teacher / trusted staff member, or an organisation such as Childline or Child Exploitation and Online Protection Command (CEOP) report abuse button

- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Enquiry Skills curriculum

- Where a student has significant learning difficulties and / or poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- The school is working towards encrypting all mobile devices issued to staff that may be removed from the school site.

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended. See following section.

- Staff must ensure they lock their screen before moving away from their computer during their normal working day to prevent unauthorised access.

- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.

- Ensure the security of any personal, sensitive, confidential and classified information contained in documents users fax, copy, scan or print. This is particularly important when shared multi-function printers are used and when access is from a non-school environment.

- Staff are to only download personal data from systems if expressly authorised to do so by their manager.

- Users must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

- Staff must keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information.

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media or internet

- Ensure removable media is purchased with encryption.

- Store all removable media securely.

- Securely dispose of removable media that may hold personal data.

- Encrypt all files containing personal, sensitive, confidential or classified data.

- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

Remote Access

- Where made available to individual staff they are responsible for all activity via a remote access facility.

- Only use equipment with an appropriate level of security for remote access

- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

- Select PINs to ensure that they are not easily guessed, eg do not use your house or telephone number or choose consecutive or repeated numbers.

- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

Social Media, including Facebook, and Twitter, Instagram and SnapChat

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Twitter to communicate with parents and carers. The website administrator is responsible for all postings on these technologies and monitors responses from others.

- Staff are not expected to access their personal social media accounts using school equipment during school hours.

- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach students the safe and responsible use of Social Media.

- Students are not permitted to access their social media accounts whilst at school.

- Students in Years 12 & 13 are permitted to access their personal social media account using their own device (i.e. mobile phone) outside of lessons.

- Staff, students, parents and carers are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

- Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

- Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

MONITORING AND EVALUATION

The policy is monitored by the various responsible IT personnel (named in the policy) in liaison with the Head. Any development of the policy will be discussed by the Governors Curriculum Committee, thereafter, ratified by the Full Governing Body.