ICT ACCEPTABLE USE POLICY

AIM/PURPOSE

The aim of this policy is to ensure that all users of ICT associated with Trinity are clear about its acceptable use. ICT 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 and Communications 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 ICT 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 and Twitter

- 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 ICT, 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 pupils 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. The loss of sensitive information can result in media coverage and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

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 should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement 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, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

ACCEPTABLE USE POLICY AT TRINITY CHURCH OF ENGLAND HIGH SCHOOL

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification and contact their department.

ICT authorised 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 its employees 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 ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised 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 business-related issues retained on that account.

Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT 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.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:
- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take, or refrain from taking, steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

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

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT 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 ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are: Deputy Head (Student Support), Systems Manager and Business Manager.

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools'

eSafety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has 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.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is *Deputy Head (Student Support)* who has been designated this role as a member of the senior leadership team. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance.

Senior Management and governors are updated by the Head/ eSafety co-ordinator and governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils 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 in Enquiry Skills lessons

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

- 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 Cybermentors, Childline or 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

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

- You 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 colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

- 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 Systems 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 e-safety coordinator or teacher as appropriate

- It is the responsibility of the school, by delegation to the Systems 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 System Manager's to install or maintain virus protection on personal systems.

- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from *the Systems Manager*

- If there are any issues related to viruses or anti-virus software, the Systems 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.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school

- 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)

- Our 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

- Our students are asked to report any incidents of Cyberbullying to the school

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school 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 http://www.coppa.org/comply.htm

Personal or Sensative Information

Protecting Personal, Sensitive, Confidential and Classified Information

- 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.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You 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

- Keep your screen display out of direct view of any third parties when you 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 labeling

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

- 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

- You 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

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging 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 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

Social Media, including Facebook and Twitter

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 pupils 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

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you

- Ensure you remove portable media from your computer when it is left unattended

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC 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, 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 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 you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

Acceptable Use Agreement: Students

- I will only use ICT systems in school, including the internet, e-mail, digital video,

and mobile technologies for school purposes

- I will not download or install software on school technologies
- I will only log on to the school network, other systems and resources with my own user name and password
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher
- I am aware that when I take images of students and/or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and occasions when I am in school uniform or when representing the school
- I will ensure that my online activity, both in and outside school, will not cause my school, the staff, students or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacte

Dear Parent/ Carer

ICT including the internet, e-mail, mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with Head of Computing.

Please return the bottom section of this form which will be kept on record at the school

----

Parent/ carer signature
We have discussed this document with……………………………………………..(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Trinity Church of England High School.

Parent/Carer Signature …….………………….………………………….

Student Signature ………………………………………………………………..

Form …………………………………. Date ………………………………

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Deputy Head (Student Support) or Systems Manager.

➢ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head.
➢ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
➢ I will ensure that all electronic communications with students and staff are compatible with my professional role
➢ I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to students
➢ I will only use the approved, secure e-mail system(s) for any school business
➢ I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop or memory stick
➢ I will not install any hardware or software without permission of the Systems Manger
➢ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
➢ Images of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy.
➢ Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head
➢ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
➢ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head
➢ I will respect copyright and intellectual property rights
➢ I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute
➢ I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies
➢ I understand this forms part of the terms and conditions set out in my contract of employment

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school
Signature …….……………….….………… Date ……….………….

Full Name …….…………………………...(printed)

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.

- Never interfere with any anti-virus software installed on school ICT equipment.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the school Systems 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 ICT Acceptable Use

- Staff have read the relevant guidance documents available on the SITSS website concerning 'Safe Handling of Data' (available on the grid at - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata)

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

- Staff should avoid leaving any portable or mobile ICT 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 ICT 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 mopiers (multi-function print, fax, scan and copiers) are used

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

Disposal of Redundant ICT Equipment

- All redundant ICT 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 ICT 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 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 ICT equipment including a record of disposal

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

Email

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 pupil based, within school or international. 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 your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act. You must therefore actively manage your 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 you access your 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

- Use your own school e-mail account so that you 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 your network 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

MONITORING AND EVALUATION

The policy is monitored by the various responsible ICT 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.