TAVISTOCK COLLEGE

POLICIES & PROCEDURES

TITLE: E-SAFETY AND ICT ACCEPTABLE USE POLICY

MODEL POLICY STATEMENT

This **is** a Local Authority model policy

Local changes **have** been made to the model policy by the College (not applicable)

The model policy used is Babcock version 21012

Policy Owner:	**Vice Principal (Inclusion)**	**Review period:**	**Bi-Annual**
Last Review:	**November 2016**	**Approving Committee:**	**Curriculum 08 November 2016**
Next Review:	**Autumn Term 2018**	**Latest FGB adoption:**	**07 December 2016**

IMPACT OF THIS POLICY

The impact of this policy can be seen in the student and staff every day practice. Monitoring of cyber bullying and e-safety issues are monitored and regular assemblies take place to raise student and staff awareness of the issues.

Introduction

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, schools 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 children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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.

At Tavistock College, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people 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 to an individual. 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 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 (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Filtered Internet wireless service is provided for use by Tavistock College staff members, students and guests only. Students, staff and guests are expected to act in a professional, responsible, ethical and legal manner when utilizing the Tavistock College Wireless Network. Users must agree to the Tavistock College terms listed below:

1. Tavistock College makes no warranties of any kind, whether express or implied, for the network or technology services provided. The college is not responsible for any damages incurred including loss of data resulting from data delivery delays, missed deliveries, or financial obligations incurred through the use of Internet websites. Use of any information obtained through the Wireless Network is at the user's risk. The college disclaims responsibility for the accuracy or quality of information obtained through the Internet or other forms of electronic communication.

2. Tavistock College will not be held responsible for any physical damage, loss or theft of personal devices or for data loss. The college is not responsible for providing power to personal devices on the Wireless Network.

3. Tavistock College's Wireless Network will provide filtered Internet access only. No access to internal-only college printers, servers or services is provided.

4. Tavistock College filters, logs and monitors access to the Internet and blocks offensive, obscene, and inappropriate images and content including pornography.

5. The College reserves the right to log, monitor and review all activities on the Tavistock Wireless Network.

6. Tavistock College reserves the right to inspect, at any time, any personally owned device while connected to the Wireless Network.

7. Student use of personal electronic devices in the classroom setting will be at the discretion of the classroom teacher and building principal.

8. Tavistock College does not provide technical support for staff, student or guest personal devices on the Tavistock College Wireless Network.

9. Illegal use of the Tavistock College Wireless Network, intentional deletion or damage to files or data belonging to others, copyright violations or theft of services may be reported to the appropriate legal authorities for possible prosecution.

10. Violation of any of the above terms or to the provisions in the Tavistock College Acceptable and Responsible Use of Network Resources policy will result in the suspension or termination of a user's privilege to technology resources, a restriction of the user's privileges and a withdraw of privileges to the Tavistock College Wireless Network. Staff and students should understand that if they commit any violation of this policy, their access privileges will be suspended or revoked, disciplinary action will be taken, and/or appropriate legal action may be instituted.

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 badge. Any ICT authorised staff member will be happy to comply with this request.

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 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.

The designated Safeguarding lead may monitor student and staff use of school owned ICT equipment for Safeguarding purposes and in order to ensure that pupils and staff are safe.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedures.

Policy breaches may also lead to criminal or civil proceedings.

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 Senior Information Risk Owner (SIRO) or e-Safety Co-ordinator. 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 your Senior Information Risk Owner who is the Strategic Business Leader

Acceptable Use Agreement: Pupils - Secondary

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools 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 pupils, teachers or others are 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.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Principal – Mrs Sarah Jones.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend 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 on request to 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 will be contacted.

- School logo and details

Dear Parent/ Carer

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

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher, or the Vice Principal, or our e-Safety coordinator.

Please return the bottom section of this form to your son/daughter's tutor for filing.

✂----------

Pupil and Parent/ carer signature
We have discussed this document and …….....(pupil name) agrees to follow the e-Safety rules and to support the safe and responsible use of ICT at Tavistock College.

Parent/ Carer Signature ……..…….

Pupil Signature…….

Form …… Date …….

Acceptable Use Agreement: Staff, Governors and Visitors

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 Barbara Manning, the e-Safety coordinator or Mrs Alison Horn Senior Information Risk Owner.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- 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 pupils, parents, outside agencies and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- 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 or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the ICT support team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend 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 the Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils 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 Tavistock College.

Signature …….…….…… Date ……

Full Name ……..(printed)

Job title . . . . . .

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB, CD) must be checked for any viruses using school provided anti-virus software before using them

- Never interfere with any anti-virus software installed on school ICT equipment that you use

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

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

E-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. 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 that staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experience in sending and receiving e-mails.

Managing e-Mail

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

- It is the responsibility of each account holder to keep the 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 all school business

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

- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder

- 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 pupils are advised to cc. the Headteacher, line manager or designated account

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision 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 2000. 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 pupil e-mail users are expected to adhere to the generally accepted rules of netiquette 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, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform (the e-Safety co-ordinator/ line manager) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Scheme of Work
- However when 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 Section E-mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)
- 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
- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail
- 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
- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)

- 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

E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted

- Where your conclusion is that e-mail must be used to transmit such data:

  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Constabulary

- Partnership Trust

There is currently a review taking place on the way e-mails are sent whereby all such communications are sent using GCSx.

GCSx stands for the Government Connect Secure eXtranet. It provides a more secure communications system (i.e. more secure than the internet).

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

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

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

E-Safety

E-Safety - Roles and Responsibilities

As e-Safety 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 e-Safety co-ordinator in this school is the Vice Principal who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as SWGfL, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

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

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and Behaviour for Learning (including the anti-bullying) policy and PSHE.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The school has a framework for teaching internet skills in Computing & PSHE lessons as well as through Assemblies and tutor time.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum
- Pupils 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
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils 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 CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teaching models, discussions and via the Computing curriculum.

E-Safety Skills Development for Staff

- Our staff receive regular information and training on e-Safety issues in the form of Assemblies and bespoke CPD training sessions.
- Details of the ongoing staff training programme can be found in the CPD Folder on the shared area.
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas
- All staff are aware of the relevant legislation when using the internet, such as Data Protection and Intellectual Property which may limit what they do, but serves to protect them

Managing the School e-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The e-Safety policy will be introduced to the pupils at the start of each school year
- E-Safety posters will be prominently displayed

Incident Reporting, E-Safety Incident Log & Infringements

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 SIRO or e-Safety Co-ordinator. 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 your Senior Information Risk Owner.

E-Safety Incident Log

Some incidents may need to be recorded in other places, such as Solero, if they relate to a bullying or racist incident.

This can be downloaded http://www.thegrid.org.uk/eservices/safety/research/incident.shtml

Misuse and Infringements

Complaints
Complaints and/ or issues relating to e-Safety should be made to the e-Safety co-ordinator or Principal. Incidents should be logged and the **Flowcharts for Managing an e-Safety Incident** should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct through their contract of employment and regular CPD opportunities.

Flowcharts for Managing an E-Safety Incident

http://www.thegrid.org.uk/eservices/safety/research/incident.shtml

Exemplar flowchart to support decisions related to an eSafety incident

Following an incident the e-Safety Co-ordinator and/or Headteacher will need to decide quickly if the incident involved any illegal activity

If unsure that the incident has any illegal aspects, contact School PCSO

Users must know to switch off the monitor or close their laptop if they find anything unpleasant or frightening, and talk to a member of staff or the e-Safety Co-ordinator

Illegal may mean:

- Downloading child pornography
- Passing on to others images or video containing child pornography
- Inciting religious or racial hatred
- Extreme cases of cyberbullying
- Promoting illegal acts
- Stealing images or content for personal gain or illegal re-use (eg pirating, copyright, use of intellectual property)

Illegal activity found or suspected

The incident did not involve any illegal activity
RECORD IN THE SCHOOL INCIDENT LOG AND KEEP ANY EVIDENCE

Inform SCOMIS and the Police. Follow any advice given by the police, otherwise:
Confiscate any laptop or other device and if related to school network disable the account.
Save ALL evidence but DO NOT view or copy. Let the police review the evidence.
If a pupil is involved, inform the MASH 0345 1551071
If a member of staff is involved, inform the Local Authority Designated Officer for Allegations Management (LADO) 01392 384964

If a member of staff has behaved in a way that could have harmed a child, possibly committed a criminal offence, or behaved in a way that suggests/he is unsuitable to work with children, contact the Local Authority Designated Officer for Allegations Management (LADO) 01392 384964
If the incident does not satisfy criteria of DSB, then:

- Review evidence and decide whether accidental or deliberate
- Follow school disciplinary process

Member of staff involved ?

YES

YES OR NO

Pupil involved ?

AS VICTIM

In-school action to support the pupil, by at least one of the following:
Class teacher
e-Safety Co-ordinator
Senior Leader or Principal
Designated Senior Lead for Child Protection (DSL)
School PCSO

Inform parent/carer as appropriate
If child at risk, inform MASH immediately
Confiscate the device

AS INSTIGATOR

Review incident and ascertain if others were involved
Decide appropriate sanctions and/or support based on school rules and guidelines
Inform parents/carers if serious or persistent incident
In serious incidents consider informing MASH as the pupil could be at risk
Review school policy and procedures to inform best practice

Internet Access

The internet is an open communication medium, available to all, 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 use of the **Grid for Learning** (SWGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

The use of school systems may be monitored for safeguarding purposes, using confidential software installed for this purpose.

Managing the Internet

- The school monitors students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- 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 its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed

It is at the Principal's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- The Local Authority has a monitoring solution via the Grid for Learning where web-based activity is monitored and recorded

- School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml

- Tavistock College is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

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

- The school does not allow pupils access to internet logs

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

- If staff or pupils 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 network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Pupils 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 is it the network managers to install or maintain virus protection on personal systems.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Principal and / or Network Manager.

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

Managing Other Web 2 Technologies

Web 2, 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 pupils 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 sites to pupils within school
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils are asked to report any incidents of bullying to the school
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Principal
- The College cannot be held responsible for activities carried out using equipment that bypasses the College internet provision (i.e. 3G, 4G).

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

- Parents/ carers are expected to sign a Home School agreement containing the following statement or similar

  → **We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community**

- The school disseminates information to parents relating to e-Safety where appropriate in the form of;

  - Information and celebration evenings
  - Posters
  - Website
  - Newsletter items

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must contain a minimum of six characters and be difficult to guess
- User ID and passwords for staff and pupils who have left the School are removed from the system within 1 week.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. From Year 7 they are also expected to use a personal password and keep it private
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is

6pm.

- In our school, all ICT password policies are the responsibility of the Network Manager and all staff and pupils are expected to comply with the policies at all times

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in their personnel file

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site

- in the school prospectus and other printed publications that the school may produce for promotional purposes

- recorded/ transmitted on a video or webcam

- in display material that may be used in the school's communal areas

- in display material that may be used in external areas, ie exhibition promoting the school

- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or

electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents (if applicable) in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Manager has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform
- Our College Webmaster James Littlejohns has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Senior Leadership Team (SLT) and those authorised by SLT. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults

For further information relating to webcams and CCTV, please see http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their Unit
    - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical

and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

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. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. 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. Under no circumstances does the school allow a member of staff to

contact a pupil or parent/ carer using their personal device

- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent

- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. 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 PDAs for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Smile and Stay Safe Poster

e-Safety guidelines to be displayed throughout the school

MILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Telephone Services

Mobile Phones

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)
- Report the loss or theft of any school mobile phone equipment immediately
- The school remains responsible for all call costs until the phone is reported lost or stolen
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default
- You must not send text messages to premium rate services
- In accordance with the Finance policy on the private use of School provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a

position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

APPENDIX

A. INTRODUCTION

Social media is the term commonly given to web-based tools which allow users to interact with each other in some way- by sharing information, opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation and engagement.

This includes blogs, message boards, social networking websites (such as facebook, google+, twitter, bebo, MySpace), content sharing websites (such as flickr, YouTube) and many other similar online channels.

This policy applies to all employees within schools where this policy has been adopted. It also applies to all governors and volunteers undertaking work on behalf of the organisation. Schools should ensure contractors and agency workers are also aware of this policy. These groups will be collectively referred to as 'individuals' within this policy.

All individuals should be aware of their own conduct and behave in a manner which ensures and promotes acceptable behaviour in relation to their individual use of social media sites.

B. PRINCIPLES AND EXPECTATIONS

B.1. Other related policies

There are other policies, including those listed below which govern employee behaviour in schools with respect to the disclosure of information online, including personal activities. All individuals within schools should make sure that they are familiar with these policies:

- Data Protection Policy
- Personal Information Security Policy
- Conduct Policy for Schools
- Social Media and Online Participation Policy and Guidelines
- Setting the Standards for Acceptable Behaviour Policy
- GTC Code of Conduct and Practice for Registered Teachers (for teaching staff only)
- Safer Working Practice For The Protection Of Children And Staff In Education Settings
- Acceptable Behaviour Policy
- Equality Policy

B.2. Individuals are responsible for their own actions

School employees are encouraged to use the ICT systems they have at their disposal to enhance their work and learning opportunities for students' learning. The school, in turn, will expect its staff and volunteers to agree to be responsible users, exercising sound judgement and common sense.

Individuals should bear in mind that anything they post online, at work and at home, can potentially affect the reputation of the school and is ultimately the responsibility of the employee.

Individuals should ensure that privacy and security settings are set and used on all devices. All passwords should conform to the Password Policy, available on the Source.

B.3. Be aware of working and personal lives overlapping

Online, an employee's personal and working lives are likely to overlap. Whilst the school understands that many individuals use social media sites, it is important to remember that information/comments/images posted online originally intended just for friends and family can be forwarded on and might be viewed by students, parents and colleagues as well as members of the wider community. Be aware of
your language and conduct while on these sites, the rules governing staff conduct such as the Policy for Setting the Standards of Acceptable Behaviour and the Schools' Conduct Policy still apply.

Individuals should not accept pupils/students as 'friends' on social media sites.

If individuals have specific reasons for needing to communicate with students via a social media site they should first discuss this, with their reasons, with their line manager. Individuals must use their professional determination to set appropriate boundaries and if s/he is uncertain, to seek advice from the line manager **before** communicating with pupils/students.

Your conduct must not adversely affect the school's public image nor bring the school into disrepute. This requirement extends to when individuals use social media sites outside normal working hours. It is important that individuals should ensure that their security settings are set appropriately, including those on personal social media sites, so that individual's own sites can only be accessed and used by those approved by that individual. Any information displayed on individual's accounts are deemed to be their responsibility

B.4. Participation in a public forum

Participation in a public forum must be professional. Individuals should make sure they always act in an honest, accurate, fair and responsible way at all times. Be aware of language and conduct while on these sites, the rules governing staff conduct such as the Policy for Setting the Standards of Acceptable Behaviour and the Schools' Conduct Policy still apply.

When an employee participates in a public forum as part of their job they should specify their job title and ensure his/her line manager is aware of the discussion.

When an employee participates in a public forum as a private individual they must make that clear and only use their private e-mail address.

B.5. Consider carefully anything said/posted

Individuals are personally responsible for their words and actions. An individual must ensure that any confidential and/or sensitive information is not posted. Individuals must not make any derogatory, untrue or discriminating comments about the school, its pupils/students or other employees. Neither should any comments be made that are likely to affect the reputation of the school.

Confidential information, including information which is available to an employee due to the nature of their job, but is not in the public domain, should not be disclosed unless specific permission has been granted to do so

The College Twitter account will be managed by the Assistant Principal, who will ensure that tweets are not shared inappropriately and cannot be commented on or re-tweeted in ways which may prove injurious to staff, students and the College.

If there is any doubt, do not post it.

B.6. Do not respond to negative comments posted online

If negative or disparaging comments about the school, its pupils/students and/or other individuals with connections to the school, are posted online or by third parties to try to spark negative conversations, individuals must not respond and should bring this to the attention of their manager.

B.7. Know that the Internet is permanent

As soon as information is published online, it is essentially part of a permanent record, even if it is removed or deleted later or attempts are made to make itanonymous. Information can be disseminated very quickly via social media and is virtually impossible to retract once it has been published; even if it has beenonline for only a short time, it may well have been picked up and copied and/or forwarded on by computers around the world.

C. STANDARDS OF BEHAVIOUR

The school is committed to making the best use of all available technology and innovation to improve the way it works. However, individuals must use all forms of social media with extreme care, together with sound judgement and common sense.

Failure to adhere to this policy and those policies listed at paragraph 1 may result in formal action within the School's Conduct Policy for Employees and other appropriate action in relation to governors, volunteers, etc.

In some circumstances, inappropriate communications may result in a police investigation.

D. USE OF SOCIAL MEDIA AT WORK

The use of school-owned laptops/computers/electronic devices to access social media sites for personal use is permitted where such use is restricted to lunch- breaks and usage is reasonable and appropriate.

Employees bringing personal electronic equipment in school, such as laptops/notebooks/hand held devices need to be aware that it is at the risk of the employees and the school will not be responsibility for the safekeeping of any such devices. Personal use of these devices must also be restricted to lunchbreaks.

Employees should note their contractual responsibility to devote their time fully to their work during

paid hours. The Schools' Conduct Policy will be used to investigate any concerns regarding any employee found to be using electronic equipment for personal use during working hours, the outcome of which may lead to disciplinary action up to and including dismissal. As part of any such investigation, the school will check the employee's internet usage and will retain this information as appropriate.

E. SUMMING UP

Be aware of your association with the school and Devon County Council in online spaces. If identified as an employee or adult associated with the school and/or Devon County Council, ensure your profile is appropriate and related content is consistent with professional expectations.

- Be aware of language and professional conduct.
- Be aware of issues such as libel, defamation and slander.
- Do not breach copyright
- Never share confidential or sensitive information

- Inform senior management if participating online in a professional capacity.
- Individuals should alert senior management immediately if anything has been posted, inadvertently or otherwise, may cause issues for individuals and/or the school.