TREVIGLAS COMMUNITY COLLEGE

ICT

Introduction

Information and Communications Technology (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, colleges 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
- 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 with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

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, usually 13 years.

At Treviglas Community College, we understand the responsibility to educate our students on ESafety and Digital Literacy 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 college. This can make it more difficult for a college to use technology to benefit learners.

Everybody in the college 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 Usage Policy (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the college (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto college premises (such as laptops, mobile phones and other mobile devices).

**In the context of this policy 'staff' refers to members of staff, contracted staff through a third party and governors. This includes SCITT trainees and supply teachers.*

Monitoring

Authorised ICT staff (Pete Botterill (Network Manager) and the ICT Technician team) and members of the Senior Leadership Team may inspect any ICT equipment owned or leased by the college at any time without prior notice. Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet/Moodle, printing and photocopying 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 college business related information; to confirm or investigate compliance with college policies, standards and procedures; to ensure the effective operation of college 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.

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. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using the college 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 college employee, contractor or student may result in the temporary or permanent withdrawal of college ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the college Disciplinary Procedure. 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 SLT team or ICT. 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 Pete Botterill.

Acceptable Usage Policy:

Refer to the Home College Agreement and also Acceptable Usage Policy (Appendix 1).

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;

- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The college reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes 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.

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.

Protection of Children Act 1978

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 a 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

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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the college context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The college is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the college site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance -
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:
http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be from a trusted source checked for any viruses.

- No member of staff must interfere with any anti-virus software installed on college ICT equipment
- Any machine not routinely connected to the college network, must have provision made for regular virus updates through the ICT technician team
- If a member of staff suspects there may be a virus on any college ICT equipment, they must stop using the equipment and contact the ICT technician team

Data Security
The accessing and appropriate use of college data is something that the college takes very seriously. The college gives relevant staff access to its SIMs, with a unique username and password. It is the responsibility of everyone to keep passwords secure. Staff must keep all college 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 out of sight. Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under 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 expecting a confidential or sensitive fax should notify the sender before it is sent.

Any information that is sensitive is protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data.

Disposal of Redundant ICT Equipment Policy
- All redundant ICT equipment will be disposed of through an authorised agency. This will 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
- The college maintains a comprehensive inventory of all its ICT equipment including a record of disposal. The college's disposal record will include:
- Date item disposed of
- Authorisation for disposal, including:
  - verification of software licensing
  - any personal data likely to be held on the storage media? *
- How it was disposed of e.g. waste, gift, sale
- Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

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

e-Mail
The use of e-mail within most colleges is an essential means of communication for both staff and students. In the context of college, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including the provision of direct written contact between colleges on different projects, be they staff based or student based, within college or international

Managing e-Mail

- The college gives all staff and governors their own e-mail account to use for all college 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
- 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 college email account should be the account that is used for all college business
- Under no circumstances should staff contact students, parents, carers or conduct any college business using personal e-mail addresses
- The college has a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the college
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on college headed paper
- Students may only use college approved accounts on the college system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of a college role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Every member of staff must actively manage their e-mail account by deleting all e-mails of short-term value and organising 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 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
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform the Headteacher or Deputy Headteachers if they receive an offensive e-mail
- Students are introduced to e-mail as part of the ICT Scheme of Learning
- However college emails are accessed (whether directly, through webmail when away from the office or on non-college hardware) all the college 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
- Staff are to use their own college e-mail account so that they are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- College e-mail is not to be used for personal advertising

Receiving e-Mails
- Emails must be checked regularly
- Attachments must not be opened from an untrusted source; always question the content even if the sender is known to you, if unsure consult Pete Botterill first.
- Email systems must not be used to store attachments. All business related work must be attached and saved 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
Where an e-mail must be used to transmit such data, obtain express consent from the Headteacher or Deputy Headteacher to provide the information by e-mail. Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Encrypt and password protect
- 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 anybody/person whose details have not been separately verified (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

Equal Opportunities

Students with Additional Needs
The college endeavours to create a consistent message with parents/carers for all students and this in turn should aid establishment and future development of the colleges' eSafety rules. However, staff are aware that some students may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

eSafety and Digital Literacy - Roles and Responsibilities

As eSafety and Digital Literacy is an important aspect of strategic leadership within the college, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this college is Ms E Johnson-Sterling. All members of the college community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

SLT and governors are updated by the Headteacher/Deputy Headteacher/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our college in relation to local and national guidelines and advice. This policy, supported by the college's Acceptable Usage Policy for staff, governors, visitors and students, is to protect the interests and safety of the whole college community. It is linked to the following mandatory college policies: child protection, health and safety, home–college agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHE

eSafety and Digital Literacy 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 students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety and Digital Literacy.

- The college has a framework for teaching internet skills in IT and Computing sessions
- The college also has mapped the SWGFL Secondary Digital Literacy curriculum across all subject areas including SEAL, Assemblies and other opportunities. E Safety and Digital Literacy has a 360° commitment from all faculties in the college.
- Educating students about the online risks that they may encounter outside college is done informally when opportunities arise and as part of the eSafety and Digital Literacy curriculum
- 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, modelling 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 Digital Literacy curriculum

eSafety Skills Development for Staff

Our staff receive regular information and training on eSafety

- New staff receive information on the college's Acceptable Usage Policy as part of their induction and CPD in Professional Studies regarding their own Digital Footprint.

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the college community
- All staff are required to incorporate eSafety and Digital Literacy learning and awareness within their curriculum areas
- Staff are kept up to date with current Esafety and Digital Literacy news, developments and further reading via both INSET and the Moodle Staff Room Esafety Blog.

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 Headteacher or Deputy Headteachers. 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 Pete Boterill / Dave Baron
See Appendices 3 and 4 for Report Log and Reporting Flow Chart.

Complaints
Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher or Deputy Headteachers.

Inappropriate Material
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher or Deputy headteachers
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by Pete Botterill, depending on the seriousness of the offence; investigation by the Headteacher/ Deputy Headteacher immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

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 use of the Colleges internet connections are logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up. Internet access is being monitored by software within the College ICT department.

Managing the Internet

- The college provides students with supervised access to Internet resources (where reasonable) through the college's fixed and mobile internet connectivity
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with students
- If Internet research is set for independent study, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise this work. Parents/carers will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute college software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use
- Personal, sensitive, confidential or classified information must not be posted or disseminate such information in any way that may compromise the intended restricted audience
- Names of students, others or any other confidential information acquired through a role within college must not be shared on any social networking site or other online application

- On-line gambling or gaming is not allowed
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated

Infrastructure

- College internet access is controlled through the college's web filtering service
- Our college also employs some additional web-filtering which is the responsibility of Pete Botterill.
- Treviglas Community 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 students are aware that college based email and internet activity can be monitored and explored further if required
- The college 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 college, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all college 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 college's responsibility nor the network manager's to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to the (technician/teacher) for a safety check first
- Students and staff are not permitted to download programs or files on college based technologies without seeking prior permission from (the Headteacher/ICT technician team)
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the reporting system.

Managing Other Web 2 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 college endeavours to deny access to social networking and online games websites to students within college. 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
- 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
- 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, college details, IM/ email address, specific hobbies/ interests)
- Are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Are asked to report any incidents of Cyberbullying to the college E-Safety Co-ordinator, Head of House or SLT.

Staff may only create blogs, wikis or other online areas in order to communicate with students using the college Moodle VLE or other systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of college and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. Parents/carers are:

- Actively encouraged to contribute to adjustments or reviews of the college eSafety policy by (state how)
- Asked to read through the Acceptable Usage Policy on behalf of their child on admission to the college
- Required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g.on college website)
- Expected to sign a Home College agreement to confirm that they will support the college approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the college community.

The college disseminates information to parents/carers relating to eSafety where appropriate in the form of;

- Information and celebration evenings
- Parent focus evenings
- Practical training sessions e.g. How to adjust the Facebook privacy settings
- Posters
- College website

Passwords and Password Security

Passwords

- All staff must use personal passwords that are as secure as possible (longer passwords with a mixture of alpha numeric are preferable)
- All personal passwords must be entered every time a member of staff logs on
- Passwords should not be entered by any automated logon procedures
- Staff must change temporary passwords at first logon
- Staff must 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
- Personal passwords can only be disclosed to authorised ICT technician team when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- A member of staff must never tell a child or colleague their password
- If there is a breach of security with a password or account, inform the Headteacher or Deputy Headteacher immediately
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and students who have left the college are removed from the system within one week

If any member of staff thinks a password may have been compromised or someone else has become aware of it then report this to the IT team

Password Security

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

- Users are provided with an individual network, email, Moodle and SIMs log-in username (relevant staff). From Year 7 they are also expected to use a personal password and keep it private
- Students are not allowed to deliberately access on-line materials or files on the college network, of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the college networks, SIMs systems and/or Moodle, 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 lock on a machine for the college network is 5 minuets
- Due consideration should be given when logging into the college learning platform, Moodle or other online application to the browser/cache options (shared or private computer)
- In our college, all ICT password policies are the responsibility of Pete Botterill and all staff and students are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the college and therefore no longer have authorised access to the college's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the college has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorised access

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information. All staff must:

- ensure that any college information accessed from a m.o.s' own PC or removable media equipment is kept secure
- screens are locked when leaving a computer during the normal working day to prevent unauthorised access
- ensure the accuracy of any personal, sensitive, confidential and classified information that is disclosed or shared 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 that are faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-college environment
- only download personal data from systems if expressly authorised to do so by a member of the leadership team and ensure the device is suitably encrypted.
- 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 their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information
- ensure hard copies of data are securely stored and disposed of after use

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

- Ensure removable media is encrypted and use the college Trucrypt facility
- 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

All staff must:

- be responsible for all activity via your remote access facility
- only use equipment with an appropriate level of security for remote access
- prevent unauthorised access to college 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, e.g. 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 college 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-college environment

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 college community or public, without first seeking consent and considering the appropriateness. With the written consent of parents/carers (on behalf of students) and staff, the college permits the appropriate taking of images by staff and students with college equipment

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, 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 college's network and deleted from the staff device. Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Headteacher. Students and staff must have permission from the Headteacher or Deputy Headteachers before any image can be uploaded for publication

Consent of Adults Who Work at the College
Permission to use images of all staff who work at the college is sought on induction and a copy is located in the personnel file

Publishing Student's Images and Work
On a child's entry to the college, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the college web site
- in the college prospectus and other printed publications that the college may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the college's learning platform or Moodle
- in display material that may be used in the college's communal areas
- in display material that may be used in external areas, ie exhibition promoting the college
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

The consent form is considered valid for the entire period that the child attends this college unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents/carers, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents/carers in order for it to be deemed valid. Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published.

Storage of Images

- Images/ films of children are stored on the college's network
- Students 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 students within the confines of the college network or other online college resource

Webcams and CCTV

- The college uses CCTV for security and safety. The only people with access to this are ICT technician team and the senior leadership team. Notification of CCTV use is displayed at the front of the college
- Publicly accessible webcams are not used in college
- Webcams in college are only ever used for specific learning purposes, never using images of children or adults
- Misuse of the webcam by any member of the college community will result in sanctions
- Refer to College CCTV Policy

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the college
- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the college
- The college keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within college
- The college conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

College ICT Equipment

- As a user of the college ICT equipment, all staff are responsible for their activity
- Visitors will not be allowed to plug their ICT hardware into the college network points (unless special provision has been made). They will be directed to the wireless ICT facilities if available
- All ICT equipment is kept physically secure
- No unauthorised access or unauthorised modifications to computer equipment, programs, files or data is permitted. This is an offence under the Computer Misuse Act 1990
- Data must be saved on a frequent basis to the college's network. Staff are responsible for the backup and restoration of any data that is not held on the college's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- A time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a college network unless permission is obtained from Pete Botterill beforehand
- On termination of employment, resignation or transfer, all ICT equipment must be returned to Pete Botterill. All details of all system logons must be provided so that they can be disabled
- It is the responsibility of all staff to ensure that any information accessed from their 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 Lorraine Hill.
- 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

All activities carried out on college systems and hardware will be monitored in accordance with the general policy
Staff must ensure that all college data is stored on the college 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 a car before starting a journey
Synchronise all locally stored data, including diary entries, with the central college 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 technician team, fully licensed and only carried out by ICT technician team
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 (including phones)

The college allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the college allow a member of staff to contact a student or parent/ carer using their personal device
Students are allowed to bring personal mobile devices/phones to college but must not use them for personal purposes within the college day. At all times the device must be switched off and kept in bags
The college 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 college community is not allowed
Users bringing personal devices into college must ensure there is no inappropriate or illegal content on the device
Permission must be sought before any image or sound recordings are made on the devices of any member of the college community
Where the college provides mobile technologies such as phones, laptops and iPads for offsite visits, only these devices should be used
Where the college provides a laptop for staff, only this device may be used to conduct college business outside of college

Removable Media

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by the ICT technician team

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure

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 college uses Facebook and Twitter to communicate with parents and carers. The PA to the Headteacher is responsible for all postings on these technologies and on Facebook and monitors responses from others
- Staff are not permitted to access their personal social media accounts using college equipment at any time during college hours

- Staff are able to setup social media accounts, using their college email address, in order to be able to teach students the safe and responsible use of Facebook or other applications
- Students are not permitted to access their social media accounts whilst at college
- Students are not permitted to access their personal social media account using their own device (i.e. mobile phone) during the college day
- Staff, governors, students, parents and carers are regularly 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

Social networking activities conducted online outside work, such as blogging, involvement in social networking sites such as Facebook, and posting material, images or comments on sites such as YouTube can have a negative effect on an organisation's reputation or image. In addition, Treviglas Community College has a firm commitment to safeguarding children in all aspects of its work. Every member of our college community with respect to their responsibilities in connection with the use of social networking sites should observe these Key Principles:

Key Principles:

- Everyone at college has a responsibility to ensure that they protect the reputation of the college, and to treat colleagues and members of the college with professionalism and respect.
- It is important to protect everyone at our college from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is a key responsibility of all members of staff and it is essential that everyone at our college considers this and acts responsibly if they are using social networking sites out of college. Anyone working in the college either as a paid employee or volunteer must not communicate with college students or their parents/carers via social networking and must not initiate Facebook friend requests from students enrolled at the college or their parents/carers.
- This policy relates to social networking outside work. Blogging and accessing social networking sites using college equipment is not permitted at any time.

The following are not considered acceptable at Treviglas Community College:

- The use of the college's name, logo, or any other published material without prior permission from the Headteacher. This applies to any published material on the internet or in written documentation.
- The posting of any communication or images which links the college to any form of illegal conduct, or which may damage the reputation of the college. This includes defamatory comments or comments that contain unacceptable language.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the college.
- The posting of any images of employees, children, or anyone directly connected with the college whilst engaged in college activities except by a designated person for agreed publicity use.

In addition to the above everyone at Treviglas Community College must ensure that they:

- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the college, or anyone at or connected with the college.
- Use social networking sites responsibly and ensure that neither their personal/professional reputation, nor the college's reputation is compromised by inappropriate postings.

- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- Do not divulge confidential information or discuss issues relating to staff or students.
- Personal contact details including email, home or mobile numbers should not be given unless the need to do so is agreed by the Headteacher.
- Do not initiate or accept a Facebook friend requests with students or parents/carers.

Potential and Actual Breaches of the Code of Conduct.
In instances where there has been a breach of the above Code of Conduct, the following will apply:

- It is the professional duty of all members of the college community to report to the Headteacher if there are any breaches to this policy at the earliest possible opportunity.
- The college will take appropriate action in order to protect the school's reputation and that of its staff, parents, carers, governors, children and anyone else directly linked to the college.
- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy, this will result in action being taken under the college's disciplinary procedure. This will be considered to be a serious disciplinary offence which is also contrary to the college's ethos and principles.

* In the context of this policy 'everyone' refers to members of staff, contracted staff through a third party, governors and anyone working in a voluntary capacity at the college.

Systems and Access
Staff must:

- be responsible for all activity on college systems carried out under any access/account rights assigned to them, whether accessed via college ICT equipment or their own PC
- not allow any unauthorised person to use college ICT facilities and services that have been provided to them
- use only personal logons, account IDs and passwords and do not allow them to be used by anyone else
- keep the screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information
- ensure the screen is locked before moving away from their computer during the normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- ensure that they logoff from the PC completely when they are going to be away from the computer for a longer period of time
- not introduce or propagate viruses
- not access, load, store, post or send from college ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the college or may bring the college or CC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the college'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)
- 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. RM and RecycleIT all offer this service.

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

Telephone Services

Staff may make or receive personal telephone calls provided:

1. They are infrequent, kept as brief as possible and do not cause annoyance to others
2. They are not for profit or to premium rate services
3. They conform to this and other relevant college policies

In addition.

- College telephones are provided specifically for college business purposes and personal usage is a privilege that will be withdrawn if abused
- All staff should be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- All staff must ensure that incoming telephone calls can be handled at all times

Printing and Photocopying

1. Must be for College use only
2. Any printing / photocopying for personal use must be via reprographics and paid for.

Activity will be monitored.

Mobile Phones

- The member of staff using the college mobile phone is responsible for the security of the college mobile phone. A PIN code must be set on the college mobile phone and it must not be leftt unattended and on display (especially in vehicles)
- Report the loss or theft of any college mobile phone equipment immediately
- The college remains responsible for all call costs until the phone is reported lost or stolen
- Staff must read and understand the user instructions and safety points relating to the use of the college mobile phone prior to using it
- College SIM cards must only be used in college provided mobile phones
- 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

Appendix 1

Treviglas Community College Acceptable Usage Policy

This document covers the set of rules that are relevant to all curriculum computer access in the college.

They are valid for ALL users of the system.

NEW: We are now monitoring attempts to install and run applications that were not installed by the college. If you attempt to run or install any application on the colleges network, a record is made of your username, the PC you were using, the application you attempted to run/install, along with the date and the time of the attempt. If you click 'I agree' when you logon to this network, you have agreed not to install applications. Users who ignore/abuse this rule will be disciplined according to the guidelines at the end of this document.

You should:

- Only access websites that are appropriate for use in college.
- Respect copyright and trademarks. (You cannot copy material
- without giving credit to the person or company that owns it.)

You must not:

- Download games or other programs from the Internet.
- Use chatlines
- Send, access or display offensive messages or pictures.
- Give your name, address, telephone number or any other personal
- information about yourself or others to anyone you write to.
- Use or send bad language.
- Intentionally waste resources thus preventing use by others.

Treviglas Community College loans you an account on the computer system(s)

The College reserves the right(s) to:

- View any/all of the contents of your account
- View/access all of your transactions across the network
- View your e-mail
- Remove your access to the account

- It is **NOT** your personal/private account
- You are **NOT** invisible
- The College can and will prosecute illegal actions

- **Illegal actions are covered by the following acts:**

- **The Data Protection Act (1988)**
- **The Computer Misuse Act (1990)**
  - Unauthorised access (e.g. using another user's username and password)
  - "hacking", "introduction of viruses"
  - Unauthorised modification of the contents of a computer (installing software in your account)

- **The Copyright, Designs and Patents Act (1988)**
  - **Copyright(computer programs) regulations (1992)**
  - **It is an offence to:**
    - Copy software unless allowed by license
    - Download copyright materials (which may include MP3's)
    - Link to a site that contains material used without permission

- **Public Interest Disclosure Act (1998)**

- **Obscene Publications Act (1959)**
  - It is an offence to sell, hire or lend material that is obscene
  - This includes publishing or downloading pornographic or other offensive material from the web

- **Telecommunications Act (1984)**
  - It is an offence to transmit messages over telecommunications systems (including computer networks) of an obscene, slanderous, threatening or annoying nature
  - This **INCLUDES** the contents of e-mail

- **Theft Act (1968)**

- **The following are <u>ILLEGAL</u>**
  - Hacking
  - Intentional introduction of viruses
  - Giving someone unauthorised access (which includes giving away your password): It is NOT your account to lend to others. Actions of another whilst using your account are YOUR responsibility.
  - Downloading/storing material that is obscene
  - Downloading illegal copies of software
  - Sending messages of an obscene, slanderous, threatening nature
  - Installation of unlicensed software

These explanations are intended to be a guide as to how the acts relate to your use of the computing or network facilities and are not a legal interpretation of those acts.

Disciplinary Action Procedures

1. **Verbal Warning**

2. **Formal written warning (*recorded for future reference*) to the user and his/her parents/guardians**

3. **Withdrawal of user account**

Damage to equipment:

Any purposeful or wilful damage (be this at a physical or software level) to or theft of equipment will be charged for at the current rate. Theft of equipment of any kind takes money away from that available to improve facilities within the college.

It is in your own interest, and the interest of other pupils within the college, that the computer equipment is treated with utmost respect.
Damage to or theft of equipment will cause hassle to you and to others.

Appendix 2 Reporting Log

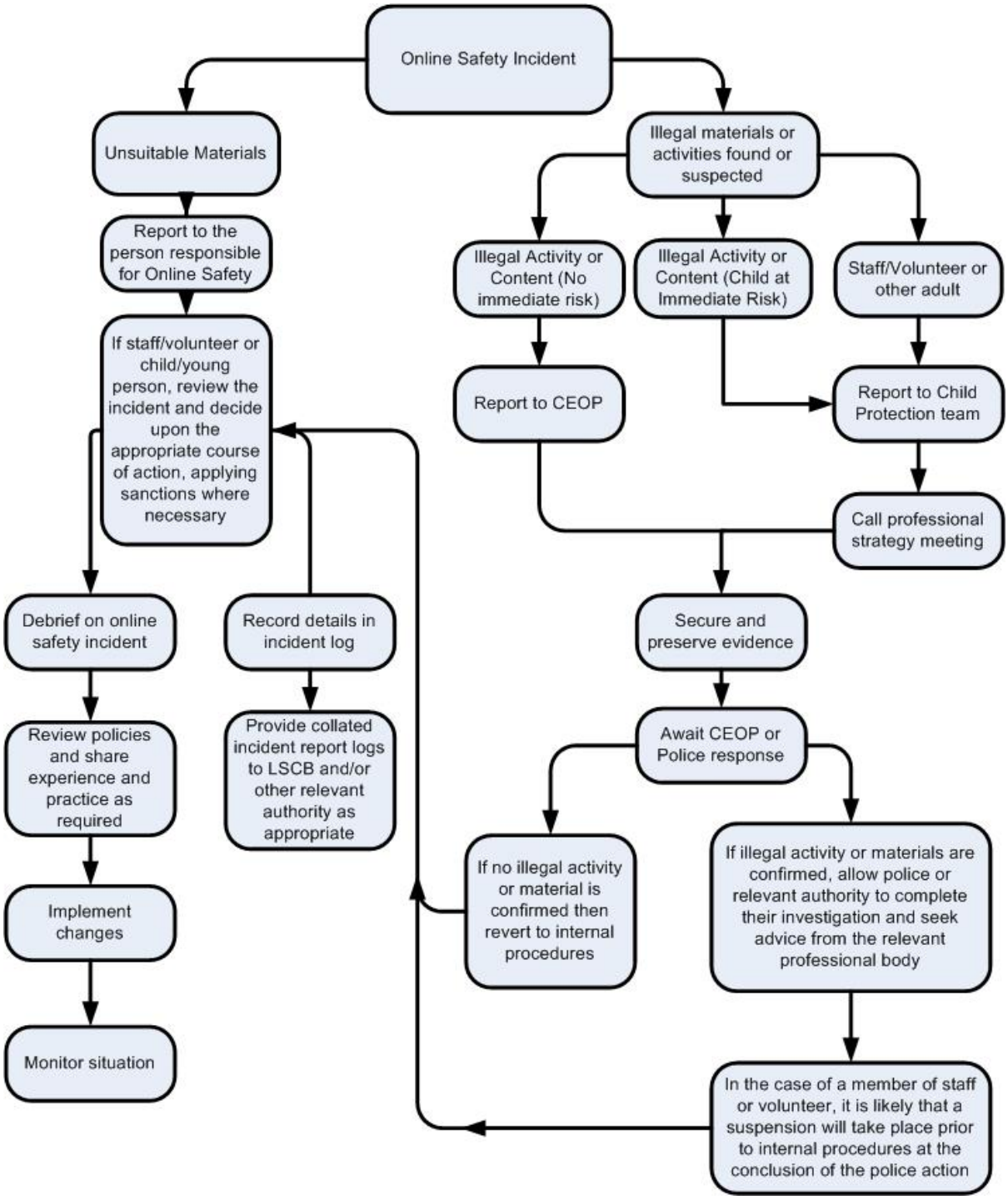
Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix 3 Reporting Procedures

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device **Reason for concern**

Conclusion and Action proposed or taken
