frome community college
specialist media arts college

E-Safety Policy

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy is designed to help to ensure safe and appropriate use. The development and implementation this strategy has involved all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore seen as essential that through good educational provision, students' resilience to the risks to which they may be exposed will be increased, so that they have the confidence and skills to face and deal with these risks.

The college must demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other ICT systems.

This e-safety policy has been developed by the E-Safety Core Group made up of the college E-Safety Coordinator (Harry Hughes), Vice Principal (Patricia Leigh), the Child Protection Officer (Gaynor Berendt) and the ICT Network Manager (Jamie Seviour). On-going consultation with the whole school community will take place through a variety of means including:

- Staff meetings, INSET Days etc
- Meetings of the E-safety group (including student representatives)
- Governors meetings
- School website / newsletters

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out annually by the Students Committee receiving regular information about e-safety incidents and monitoring reports. One governor has taken on the role of E-Safety link governor. The role of the E-Safety governor includes:

- At least one meeting per year with the E-Safety Coordinator
- Attendance at meetings of the E-Safety Group as appropriate
- Reporting to the meeting of the Students Committee as appropriate

Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Coordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinator.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Coordinator

- Leads the e-safety core group
- Along with the network manager, takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- Meets annually with E-Safety governor to discuss current issues
- Provides a report to the relevant committee meeting of governors annually
- Reports regularly to Senior Leadership Team

Network Manager

The Network Manager is responsible for ensuring:

- That the college ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- The college filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That he keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /Headteacher
- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Agreement
- They report any suspected misuse or problem to the E-Safety Co-ordinator
- Digital communications with students should be on a professional level
- Students understand and follow the school e-safety and acceptable use policy (the ICT department will take a lead on this)
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Child Protection Officer

The Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

It is recognised that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Students

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Agreement, which they will be expected to sign before being given access to college systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand college policies on the taking / use of images and on cyber-bullying
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through a variety of means eg: parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- Endorsing (by signature) the student Acceptable Use Agreement (incorporated into the student journal)
- Accessing the school website / VLE / SLP in accordance with the relevant school Acceptable Use Agreement

Community Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Education

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Young people need the help and support of the school to recognise and avoid e-safety risks.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is be provided as part of ICT and R&P curricula
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students are taught to be critically aware of the content that they access on-line and are guided to validate the accuracy of information
- Students are helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet are posted in all appropriate rooms
- Staff act as good role models in their use of ICT, the internet and mobile devices

Parents / Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's on-line experiences. Parents often either underestimate or do not realise how often young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school therefore seeks to provide information and awareness to parents and carers through a variety of means eg: the school's web site, links to useful resources and information evenings.

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of e-safety training will be made available to staff and will form part of the staff development plan
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates via the SWGfL / LA /other organisations
- The E-Safety Officer will provide advice / guidance / training as required to individuals as required

Governors

Governors will be kept informed of e-safety related issues through the Students Committee. A nominated link governor will also be supported in being able to answer questions as the need arises.

Technical

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Use Agreement and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems

Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Core Group
- All users will be provided with a username and password by the ICT Team who will keep an up to date record of users and their usernames. Users will be required to change their password on a yearly basis. Passwords must conform the password policy as detailed later in this document.
- The administrator passwords for the school ICT system, used by the Network Manager / Technical Team must also be available to the Headteacher or other nominated senior leader and will be kept in the school safe within the finance department.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report to the ICT Manager any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGFL and the internal filtering service provided by the school.
- Any filtering issues should be reported immediately to the ICT Team.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the E-Safety Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Core Group.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Users requiring “guest” access to the system need to sign a copy of the Staff AUA and pick up a username and password from reception. Student teachers also need to sign the AUA, a username and password will then be issued to them on their induction.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (see the college Data Protection Policy for further detail).

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg: on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Parents/carers are asked to inform the school if they do not wish photographs or videos to be taken of their children ie: consent is assumed unless the school is informed otherwise.
- Student's work can only be published with the permission of the student.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students			
Communication Technologies	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at certain times	Allowed with staff permiss-ion	Not allowed
Mobile phones may be brought to school	■			■			
Use of personal mobile phones in lessons			■ (except in emergency)		■	■	
Use of mobile phones and other hand-held devices in social time	■			■			
Taking photos on personal mobile phones or other camera devices			■				■
Use of personal email addresses in school, or on school network		■					■
Use of school email for purely personal reasons			■				■
Use of chat rooms / facilities			■				■
Use of instant messaging			■				■
Use of social networking sites			■				■
Use of blogs	■				■	■	

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the network manager the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, VLE etc) must be professional in tone and content.

Unsuitable / inappropriate activities

The college believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable at certain times	Acceptable for staff only	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images				■
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				■
	adult material that potentially breaches the Obscene Publications Act in the UK				■
	criminally racist material in UK				■
	pornography			■	
	promotion of any kind of discrimination			■	
	promotion of racial or religious hatred			■	
	threatening behaviour, including promotion of physical violence or mental harm			■	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			■	
Using school systems to run a private business				■	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				■	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				■	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				■	
Creating or propagating computer viruses or other harmful files				■	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				■	
On-line gambling				■	
File sharing				■	
On-line gaming (non educational)				■	
Use of social networking sites				■	
On-line gaming (educational)		■			
On-line shopping / commerce			■		
Use of video broadcasting eg Youtube			■		

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. If any apparent or actual misuse appears to involve illegal activity ie:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

then the matter will be given urgent attention by a member of the Leadership Team and/or the Child Protection Officer. The police will be informed.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Investigations into some forms of misuse (eg: accessing inappropriate on-line material) will be carried out by more than one member of staff, using a “clean” designated computer.

Incidents involving inappropriate rather than illegal misuse by students are likely to emerge relatively frequently. These incidents are dealt with as soon as possible in a proportionate manner, and members of the school community are aware that incidents have been dealt with. It is intended that incidents of such misuse will be dealt with through the normal behaviour / disciplinary procedures ranging from action by the class teacher, to the involvement of more senior staff members.

Staff – Acceptable Use Agreement

ICT Acceptable Use Agreement for Staff and Associated Adults

Introduction

All adults using ICT equipment within the school must ensure that they have read and abide by the Acceptable Use Agreement. It is also advised that all staff should make themselves aware of the school's E-Safety Policy.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That adults will be responsible users and stay safe while using the internet and other communications technologies
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk (see the college E-Safety Policy for further details)
- That staff are protected from potential risk in their use of ICT in their everyday work

The school will try to ensure that adults will have appropriate access to ICT to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect all users to agree to be responsible users.

The school runs a 'managed system' rather than a lock down system for Internet access. This means that the school in conjunction with the SWGfL provide filtering to remove the most dangerous and inappropriate types of content. We expect all staff to remind and reinforce with students the need to be careful and to 'think before they click' when using ICT in their lessons. All staff have a shared responsibility in helping to educate the students in how to remain safe and be responsible when using ICT. Just as important is helping the students to understand what to do in the event of them finding something inappropriate.

Staff need to be aware that the school's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring. They should be used primarily for school purposes but occasional personal use is permitted. All ICT activities must conform to the norms of moral decency and not contravene ICT or other relevant legislation.

ICT Acceptable Use Policy Agreement

I understand that I must use college ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I will not disclose any of my usernames or passwords to anyone else, nor will I try to use any other person's username and password
- I understand that the rules set out in this agreement also apply to use of school ICT systems out of school (eg laptops, email, VLE etc)
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use outside of directed time
- I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of, to the appropriate person

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital media. I will not retain any images on personal equipment. Where these images are published (eg on the school website/VLE) it should not be possible to identify by name, or other personal information, those who are featured
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I understand that it is not acceptable to use my personal communication accounts to contact students
- I will not communicate with any student using a personal mobile phone (voice or text). When contacting parents, wherever possible, will use a school phone and when not possible, I will endeavour to with-hold access to my personal number
- I will not engage in any on-line activity that may compromise my professional responsibilities

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will not connect any personal equipment directly to the network
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes;
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or which may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will not disclose or share personal information about any student or employee to anyone outside of the organisation. Exceptions, including the Police and social services, are outlined in the school's Data Protection Register Entry.
- Where personal data is transferred outside the secure school network, it must be done so via the SLP or by use of an encrypted memory stick and not sent by e-mail
- I will not give any student access to a PC designated for staff use
- I will immediately report any damage or faults involving equipment or software to the ICT Team, however this may have happened
- As an additional precaution to the college back-up systems, I will encourage students to save copies of important documents (eg: coursework) onto a memory stick or to the VLE

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- I will ensure that any published material which includes photographs of people, I have ensured that their permission has been sought before they are used
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). I will not take copies of any electronic media and place them onto the school system, unless the school has purchased a license to make such copies (this includes the use of personal media software such as iTunes)

When using internet technologies in my teaching:

- I understand I have a duty to remind students about appropriate and safe use of Internet technologies whenever appropriate
- I understand that I should be guiding students in their exploration of the Internet
- I understand that I should encourage the students to 'think before they click' in a bid to reduce the incidence of inappropriate content being viewed
- I understand that I have a duty to ensure the students are aware of what to do should they find something inappropriate
- I understand that I must report any breaches of ICT policy to ICT support/ the Leadership Team as appropriate
- I understand that any misuse will be dealt with seriously by a member of the Leadership Team and could have legal implications

Respect for the school's resources:

- I will not try (unless I have permission) to make large downloads (greater than 100Mb) or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not take up internet capacity by continuous streaming of live radio or live video over the Internet (outside of lessons), which has the effect of preventing others from being able to carry out their work effectively;
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings. I understand that all software is installed by the ICT support team and any plans for new software should be discussed with them before any purchase is considered
- I will not add any hardware to the system, including laptops, printers, scanners and web cams
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will endeavour to use the resources in an economical way and use the appropriate output wherever possible. I will ensure that I do not waste resources by printing multiple copies to printers, and use photocopiers instead
- I will check my email on a regular basis and clear messages so that my mailbox does not become full

Social Networking Sites

- I will not use the school resources / systems to access chat and social networking sites
- I understand that the school strongly advises that I carefully consider and regularly review the privacy settings on any social networking site I am a member of and that I act to protect my professional identity online
- I will not have any photographs or statements on public view that I would be ashamed to put on a school notice board
- I will not under any circumstances have any current students as 'friends' within a social networking site and understand that I am strongly advised against keeping in touch with ex-students in this way (particularly if they are under 18 years of age)

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action

Student – Acceptable Use Agreement

ICT Acceptable Use Agreement

This policy has been written so that:

- All students can enjoy the very best access to ICT including the Internet
- All students will become responsible and safe users
- The college ICT systems are protected from accidental or deliberate misuse

For my own personal safety:

- I understand that the college will monitor my use of all the ICT systems, including e-mail and printing

  I understand that computer storage areas and memory sticks (including those brought in from home) cannot be regarded as completely private
- I will not share my own username and password and will never try to use anyone else's
- I will immediately report to the teacher any unpleasant or inappropriate material or messages that make me feel uncomfortable, including mobile phone communications
- I will be aware of "stranger danger" when I am communicating on-line and will not share my personal details with anyone

I will act as I expect others to act toward me:

- I will respect others' work and property and will not alter any other user's files
- I will make polite, responsible and appropriate use of electronic communications
- I will never, either in or out of school, seek to harass or abuse fellow students or members of staff through any form of electronic communication (eg: e-mail, text message or status updates on social networking sites)
- I will not take, publish or distribute images of anyone unless it is part of a lesson
- I will only use a personal hand held device (eg: mobile phone) in school at break and lunchtime or if directed to as part of a lesson. I will follow the rules in this agreement when using any personal device

When using the internet:

- I understand that using the work of others published on-line without permission will be classed as cheating by Exam Boards and may result in being excluded from exams
- I will not bring into school or try to download, upload or access copies of any material that is illegal, protected by copyright (including music, videos and games) or is inappropriate
- I will adopt a 'think before I click' routine when using the internet

Respect for the system

- I will not attempt to bypass any network or Internet security systems
- I will immediately report to the teacher any damage or faults
- I will not open any attachments to emails, unless I know and trust the sender
- I will not install or attempt to install programmes of any type nor will I alter computer settings
- I will not connect any laptop or other mobile device to the college system
- I will only print what I need to do my school work and will only print in colour when essential
- I will not use the system for playing any non-educational games
- I understand that my work area is for school work only and I will manage it to ensure it isn't full

School Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the ICT network manager. The ICT Team will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems. To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs
- be reported to a second responsible person (E-safety Coordinator)

All users have a responsibility to report immediately to the ICT Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement
- induction training
- staff meetings, briefings, INSET

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the ICT Network Manager who will decide whether to make school level changes (as above

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- E-Safety Coordinator
- E-Safety Core Group
- E-Safety Governor / Students Committee
- SWGfL / Local Authority on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision

School Password Security Policy

Introduction

The ICT Team is responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of the ICT Network Manager. All users have responsibility for the security of their username and password; they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Passwords for new users, and replacement passwords for existing users will be allocated by the ICT team. Users will be required to change their passwords every year.

Training / Awareness

Members of staff will be made aware of the college password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the college password policy:

- in ICT and / or e-safety lessons (the school should describe how this will take place)
- through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety core group.

All users will be provided with a username and password by the network manager who will keep an up to date record of users and their usernames. Users will be required to change their password every year.

The following rules apply to the use of passwords:

- the last four passwords cannot be re-used
- the password should be a minimum of 8 characters long and
- must include a uppercase character, a lowercase character and a number. Special characters can also be used
- the account will be “locked out” for 5 minutes following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- requests for password changes need to be made in person to the ICT Team to ensure that the new password can only be passed to the genuine user

The “master / administrator” passwords for the school ICT system, used by the technical team must also be available to the Headteacher or other nominated senior leader and kept in the school safe.

Audit / Monitoring / Reporting / Review

The network manager will ensure that full records are kept of:

- User IDs and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by the E-Safety Core Group annually.

E-Safety – A School Charter for Action

Name of School	Frome Community College
Name of Local Authority	Somerset

We are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential e-safety risks.

Our college community

Discusses, monitors and reviews our e-safety policy on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports staff in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole school curriculum.

Ensures that students are aware, through e-safety education, of the potential e-safety risks associated with the use of ICT and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's e-safety policy.

Provides opportunities for parents/carers to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. The school will report back to parents / carers regarding e-safety concerns. Parents/carers in turn work with the school to uphold the e-safety policy.

Seeks to learn from e-safety good practice elsewhere and utilises the support of the LA, SWGfL and relevant organisations when appropriate.

Chair of Governors	
Headteacher	
Student Representative	