



## CALLINGTON COMMUNITY COLLEGE (ACADEMY TRUST)

# DIGITAL TECHNOLOGY USE & E-SAFETY POLICY

### Overview of policy

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

This policy incorporates a number of aspects of using ICT within and outside of the College including:

- E-safety Policy
- Using Images of Children Policy
- Use of Digital Technologies Policy
- Acceptable Use Policies for Staff, Students and Parents
- Filtering Policy
- Password Policy

The use of technology has become integral to many of our lives and has certainly become part of the way we communicate and access information. 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 College's e-safety provision. Children and young people need the help and support of the College to recognise and avoid e-safety risks and build their resilience (See Appendix 2 for details about education of the safety and digital ICT use we offer).

Appendix 1 outlines the roles and responsibilities of students and staff concerning E-safety and the use of digital technology. All staff and students are required to sign Acceptable Use Policies (AUPs) in order to use digital technologies and parents provided with details of these. It is assumed that parents agree to the AUPs that their child signs as part of the whole school agreement.

### Technical – infrastructure/equipment, filtering and monitoring

#### *Infrastructure/equipment*

The College will be responsible for ensuring that the college infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- College ICT systems will be managed in ways that ensure that the college 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.

- There will be regular reviews and audits of the safety and security of college ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to college 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 Committee.

### **Filtering Policy**

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 College maintains and supports the managed filtering service provided by SWGfL.
- The responsibility for the management of the college's filtering policy will be held by the Network Manager.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Director of Elearning & Systems. Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Director of Elearning & Systems. All users have a responsibility to report immediately to the Network Manager any infringements of the college'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.
- 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 AUP, induction training, staff meetings, briefings, Inset.
- Parents will be informed of the college's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions and the College website.
- 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 Network Manager who will decide whether to make college level changes (as above). If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the Network Manager will contact SWGfL.

No filtering system can guarantee 100% protection against access to unsuitable sites. The College will therefore monitor the activities of users on the college network and on college equipment as indicated in the College E-Safety Policy and the Acceptable Use agreement. Monitoring will take place and logs of filtering change controls and of filtering incidents will be made available to the Director of Elearning & Systems, the E-Safety Committee, the E-Safety Governor & 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.

## **Password Policy**

- 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 term.
- The "administrator" passwords for the college ICT system, used by the Network Manager must also be available to the Headteacher or The Director of Elearning & Systems.
- 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 any suspicion or evidence that there has been a breach of security.
- College ICT technical staff regularly monitor and record the activity of users on the college ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity.
- Users should 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 college systems and data.
- A procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the college system. This is implemented and logged by the Network Manager.
- The Acceptable Use Policies outline the use of College ICT systems.
- The college infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data cannot be sent over the internet or taken off the college site unless safely encrypted or otherwise secured.
- The College will be responsible for ensuring that the college 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 college's personal data protection policy;
  - logs are maintained of access by users and of their actions while users of the system.
- The management of the password security policy will be the responsibility of the Network Manager
- Passwords for new users, and replacement passwords for existing users can be allocated by the ICT Technicians and will require immediate change of password.
- Members of staff will be made aware of the college's password policy at induction, through this policy and through the Acceptable Use Agreement.
- Students will be made aware of the college's password policy in ICT e-safety lessons and through the Acceptable Use Agreement.
- The Network Manager will be responsible for ensuring that full records are kept of User Ids and requests for password changes, User log-ons and 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.

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

## **E-safety and the Curriculum**

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time-to-time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

## **Use of Digital and Video Images Policy - Photographic, Video**

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 college 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 e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on college 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 college 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, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents/carers.
- Parent/carer permission is not required for students over 18 years of age as long as the picture was taken after the student turned 18.
- Images of students that have left college must not be used unless the consent of parents/carers is given.
- Names of students will not be published with any images of children without prior specific and separate consent from parents/carers.
- If a student is named in any text which the College publishes, a photograph will not be included with the text, unless this is the wish of the student and parents/carers.
- Where possible publishing close up or individual photographs of students should be avoided. The College's preference is to publish class or group images of students.
- Parents/carers of students taking part in sporting or performance activities e.g. Music, Drama, Dance should be asked to complete a more specific form relating to publicity.
- Names of students must not be passed to the press for photographs or recordings which the press wish to publish or broadcast, unless a parent/carer has consented to this.
- Written permission from parents/carers will be obtained before photographs of students are published on the college website (see **The Use of Images of Children Policy Agreement**).

## **Data Protection when using digital technology**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer personal data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be password protected and encrypted if the data stored is classed as high.
- The device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in-line with college policy (below) once it has been transferred or its use is complete

There is also a whole college Data Protection policy that covers all aspects of data protection in addition to the digital technology aspects outlined here.

## **The code of conduct for the responsible use of digital technology**

### **Hand-held devices: including mobile phones, ipods and mp3 players**

The college recognises the advantages of digital technology for staff and students as a means of communication and as a learning tool. However, this technology is open to abuse leading to the invasion of privacy and, in its most serious form, cyber-bullying. This code of conduct sets out appropriate use of digital technology while protecting the individual and maintaining a productive, working environment. We expect all students to use digital technology responsibly.

Misuse of digital technology that results in an invasion of privacy or personal distress is CYBER-BULLYING and this will not be tolerated at the college. The College will investigate any suspected cyber-bullying where there is evidence that it is causing distress to one or more students of the college. Where there is proof of cyber-bullying the bullies will be punished in the ways detailed within this code, whether or not the cyber-bullying took place on the college site.

### **Guidelines for use of mobile phones, MP3 players or I-pods**

- Students are allowed to carry mobile phones, ipods & Mp3 players.
- Students must not use mobile phones to communicate in any form during lessons.
- Mobile phones should be switched off and in bags during lessons.
- Using a mobile phone in-between lessons must not cause you to be late to a lesson.
- Students must seek permission from the class teacher to use other mobile phone tools during the lesson such as calculator or clock.
- Students must not use mobile phones when travelling between lessons.
- Students must not use MP3 players or I-pods (or similar devices) in lessons.
- In some lessons teachers may feel it is beneficial for students to use the multimedia functions of mobile phones, ipods or MP3 players. Such functions are to be used in a respectful and appropriate way.
- Mobile phones or other devices must not be used to take a photograph of anyone without their permission.
- Mobile phones or other devices should not be used to record anyone's voice without their permission.
- Mobile phones or other devices must not be used to video anyone without their permission.
- Mobile phones are banned from use in public examinations. They must not be taken into the examination room at all. The consequences of a mobile phone ringing or being found on

you in an examination are very severe and could include disqualification from that examination.

- Mobile phones are expensive items and the college will not take any responsibility for the phone if it happens to be stolen or lost whilst in college. Students bring mobile phones to college at their own risk. During PE lessons phones and other valuable items should be handed in by the student to the valuables box.
- Staff must not use mobile phones in the classroom.
- Staff must not give out personal mobile phone numbers to students or parents/carers.
- The college reserves the right to ban the possession of mobile phones on site if a student persistently misuses their phone.
- By allowing you the privilege of using mobile phones in certain circumstances in college you are expected to observe these rules.

## **Cyberbullying**

- During any investigation of suspected invasion of privacy or bullying the student concerned will be requested to show senior members of staff the contents of text messages or photos/videos contained on their phones. Full co-operation is expected and parents/carers will be involved in the investigation if the student refuses to co-operate.
- Bullying which impacts on students at the college will not be tolerated, no matter where the bullying began. Do not assume that once you leave college you can partake in bullying and be beyond punishment.
- Students found guilty of bullying or invasion of personal privacy will not be allowed to bring a mobile phone to college at all. There will also be an additional punishment depending on the severity of the incident. This could range from a detention to some type of exclusion.

## **Use of social networking sites and chatrooms**

- Chatrooms, Bebo, Myspace or similar sites are not to be used or even accessed at the college. Students are protected from access to such sites by filters. These filters are designed to prevent inappropriate contact by members of the public and are commonly used in colleges across the country. Students must not try to by-pass such filters in any way.
- Sending inappropriate messages or posting inappropriate comments about other students or teachers will result in a punishment which, in the most extreme cases, could be an exclusion.

## **Use of Email**

- The content of any e-mails to other students or teachers and the content of any messages posted on any sites on the internet should not be offensive, abusive or cause another person distress.
- The official college e-mail service may be regarded as safe and secure and is monitored.
- Users need to be aware that e-mail communications may be monitored.
- Users must immediately report, to their Head of Year or the Network Manager the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.
- Any digital communication between staff and students or parents/carers (e-mail, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) college systems (College E-mail/VLE). Personal e-mail addresses, text messaging or public chat/social networking programmes must not be used for these communications.

- Students should be taught about e-mail safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate e-mails and be reminded of the need to write e-mails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the college website and only official e-mail addresses should be used to identify members of staff.

### Consequences of misuse by students

Type of misconduct	Minimum response
Using mobile phone that causes lateness to lesson	Detention (break time or after college depending on the severity) and confiscation of mobile phone for a fixed period
Using MP3 player/I-pod in a lesson	Detention. Confiscation of MP3 player/I-pod
Mobile phone ringing in a lesson (call or message)	At least after-college detention. Mobile phone confiscated for a fixed period of time at the college's discretion
Using mobile phone to make a call/send a message in a lesson	At least one-day exclusion. Mobile phone confiscated for a fixed period of time at the college's discretion
Using mobile phone to record sounds or video without permission at any time of the day	At least one-day exclusion. Mobile phone confiscated for a fixed period of time at the college's discretion
Use of phone to make inappropriate calls/texts that are found to be bullying	At least one-day exclusion. Mobile phone confiscated for a fixed period of time at the college's discretion
Use of e-mail, social networking sites or chat rooms to make inappropriate comments about other students that are found to be bullying	At least one-day exclusion. Mobile phone confiscated for a fixed period of time at the college's discretion. E-mail account suspended for a period of time. Possible suspension of network access for serious cases.
Using Bebo, Myspace, chat rooms or similar sites or bypassing the filters put in place by the college using any method	At least an after-college detention. Serious misuse could result in an exclusion.

## Table of acceptable use for communications technology

	Staff and other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to college	√				√			
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√				√			
Taking photos on mobile phones or other camera devices	√						√	
Use of hand held devices e.g. PDAs, PSPs	√						√	
Use of personal e-mail addresses in college, or on college network		√						√
Use of college e-mail for personal e-mails		√				√		
Use of chat rooms / facilities *				√				√
Use of instant messaging *				√				√
Use of social networking sites *				√				√

\*Education use of VLE for chatroom, forums, Instant Messaging allowed. May be used by staff and students for specific educational purposes, monitored by staff and E-Safety Officer.

## Unsuitable / inappropriate activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	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, e.g. 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 college or brings the college into disrepute				√		
Using college 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 college				√		
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 (e.g. 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 gaming (educational)		√				

<b>User Actions</b>	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
On-line gaming (non educational)			√		
On-line gambling				√	
On-line shopping/commerce				√	
File sharing				√	
Use of social networking sites (*see above re VLE)				√	
Use of video broadcasting e.g. Youtube			√		

## Responding to incidents of serious misuse

It is hoped that all members of the college 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.

Listed below are the responses that will be made to any apparent or actual incidents of misuse including those that involve illegal activity i.e.:

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

## Responses to incidents of misuse

- If students suspect that inappropriate or illegal material is being accessed they must report it to the nearest member of staff immediately.
- If staff suspect that inappropriate material is being accessed they must report it to the Network Manager immediately. The Network Manager will follow SWGfL protocols as set out on their website: <http://www.swgfl.org.uk/safety/default.asp>
- If staff suspect that illegal materials are being accessed they must report it immediately to the Director or Elearning & Systems, a member of the Leadership Team or the Network Manager immediately. The computer should be unplugged from the mains but not shut down (as this preserves the evidence). The police will need to be contacted by a suitable member of the Leadership Team.
- If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

## Table of Actions following Misuse, inappropriate or illegal incidents

Students	Actions / Sanctions									
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year/other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc	Inform parents/carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention/exclusion	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		Y	Y	Y		Y	Y	Y	Y	
Unauthorised use of non-educational sites during lessons	Y	Y					Y	Y	Y	
Unauthorised use of mobile phone /digital camera/other handheld device	Y	Y				Y		Y	Y	
Unauthorised use of social networking/instant messaging/ personal e-mail	Y	Y				Y	Y	Y	Y	
Unauthorised downloading or uploading of files	Y	Y			Y	Y	Y	Y	Y	
Allowing others to access college network by sharing username and passwords	Y	Y			Y	Y	Y	Y	Y	
Attempting to access or accessing the college network, using another student's account	Y	Y			Y	Y	Y	Y	Y	
Attempting to access or accessing the college network, using the account of a member of staff	Y	Y			Y	Y	Y	Y	Y	
Corrupting or destroying the data of other users	Y	Y			Y	Y	Y	Y	Y	
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature	Y	Y			Y	Y	Y	Y	Y	

## Students

## Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year/other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc	Inform parents/carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention/exclusion
Continued infringements of the above, following previous warnings or sanctions	Y	Y			Y	Y	Y	Y	Y
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college	Y	Y	Y		Y	Y	Y	Y	Y
Using proxy sites or other means to subvert the college's filtering system	Y	Y			Y	Y	Y	Y	Y
Accidentally accessing offensive or pornographic material and failing to report the incident	Y	Y			Y	Y	Y	Y	Y
Deliberately accessing or trying to access offensive or pornographic material	Y	Y	Y		Y	Y	Y	Y	Y
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	Y	Y				Y	Y	Y	

## Staff

## Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		Y	Y	Y			Y
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging / personal email	Y	Y				Y	Y
Unauthorised downloading or uploading of files	Y	Y				Y	

**Staff**

**Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Disciplinary action
Allowing others to access college network by sharing username and passwords or attempting to access or accessing the college network, using another person's account	Y	Y				Y	Y
Careless use of personal data e.g. holding or transferring data in an insecure manner	Y	Y				Y	Y
Deliberate actions to breach data protection or network security rules	Y	Y				Y	Y
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	Y	Y				Y	Y
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature	Y	Y				Y	Y
Using personal e-mail/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	Y	Y				Y	Y
Actions which could compromise the staff member's professional standing	Y	Y				Y	Y
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college	Y	Y				Y	Y
Using proxy sites or other means to subvert the college's filtering system	Y	Y				Y	Y
Accidentally accessing offensive or pornographic material and failing to report the incident	Y	Y				Y	Y
Deliberately accessing or trying to access offensive or pornographic material	Y	Y	Y		Y	Y	Y
Breaching copyright or licensing regulations	Y	Y				Y	Y
Continued infringements of the above, following previous warnings or sanctions	Y	Y					Y

## Appendix 1: Roles and Responsibilities

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

### 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 by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Officers;
- regular monitoring of e-safety incident logs;
- regular monitoring of filtering/change control logs;
- reporting to relevant Governors committee/meeting.

### Headteacher and Senior Leaders

- The Headteacher/Deputy Headteacher is responsible for ensuring the safety (including e-safety) of members of the college community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator/Officer.
- The Headteacher/Deputy Headteacher is responsible for ensuring that the E-Safety Officers 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/Deputy Headteacher will ensure that there is a system in place to allow for monitoring and support of those in college 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 Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator/Officer.
- The Headteacher and 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 (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR/disciplinary procedures).

### E-Safety Officers

- Leads the E-safety Committee (as part of the Safeguarding committee).
- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the College 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 college ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meeting/committee of Governors.
- Reports regularly to Leadership Team.

## **Network Manager**

The Network Manager is responsible for ensuring:

- That the College's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the College 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 College'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.
- That they are kept 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/Virtual Learning Environment (VLE)/remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Officer and other relevant member of staff for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in college 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 college E-safety policy and practices.
- They have read, understood and signed the college Staff Acceptable Use Policy/Agreement (AUP).
- They report any suspected misuse or problem to the E-Safety Officer.
- Digital communications with students (e-mail/Virtual Learning Environment (VLE)/ voice) should be on a professional level and only carried out using official college systems.
- E-safety issues are embedded in all aspects of the curriculum and other college activities.
- Students understand and follow the College E-safety and Acceptable Use policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended college activities.
- 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 college policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

## **Designated Person for Child Protection**

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.

## **E-Safety Committee (part of safe-guarding Committee)**

Members of the E-safety Committee will assist the E-Safety Officers with:

- The production/review/monitoring of the College E-safety policy/documents.

## **Students:**

- Are responsible for using the college ICT systems in accordance with the Student Acceptable Use Policy, 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.
- 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 understand college 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.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of college and realise that the College's E-Safety Policy covers their actions out of college, if related to their membership of the college.

## **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. Research shows that many parents/carers do not fully understand the issues and are less experienced in the use of ICT than their children. The college will therefore take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local e-safety campaigns/literature. Parents/carers will be responsible for:

- Endorsing the Student Acceptable Use Policy;
- Accessing the college website/VLE/on-line student records in accordance with the relevant college Acceptable Use Policy.

## **Community Users**

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

## **Appendix 2: E-safety and digital technology use education and training for students, staff, parents/carers & governors**

### **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 college's e-safety provision. Children and young people need the help and support of the college to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety programme should be provided as part of ICT/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in college and outside college.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be helped to understand the need for the student Acceptable Use Policy (AUP) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside college.
- Students should be 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 will be posted in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

### **Parents/carers**

Many parents/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/regulation of the children's on-line experiences. Parents/carers often either underestimate or do not realise how often children and 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 College will therefore seek to provide information and awareness to parents/carers through:

- Letters, newsletters, website, VLE.
- Parents evenings.
- Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents/carers).

### **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 planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the College E-safety Policy and Acceptable Use Policies.
- The E-Safety Co-ordinator (or other nominated person) will receive regular updates through attendance at SWGfL/LA/other information/training sessions and by reviewing guidance documents released by BECTA/SWGfL/LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-Safety Co-ordinator (or other nominated person) will provide advice/guidance/ training as required to individuals as required.

## **Governors**

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in ICT/ e-safety/health and safety/ child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/SWGfL or other relevant organisation.
- Participation in college training/information sessions for staff or parents/carers.