Digital Safety and Acceptable Use Policy

Table of Contents

1. Development/Monitoring/Review of this Policy

This Digital Safety Policy has been developed by a working group made up of:

- Director of Digital Learning
- IT Network Manager
- DSL
- Digital Strategy Group
- Board of Directors

2. Schedule for Development/Review

The Implementation of this policy will be monitored by the:	Online Safety Leads (DoDL, DSL)
Monitoring will take place at regular intervals:	Annually prior to new academic year
The digital safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	May 2023

3. Aims of the Policy

Elizabeth College recognises that technology plays an important and positive role in children's lives, both educationally and socially. It is committed to helping all members of the College community to understand both the benefits and the risks of technology and to equip students with the knowledge and skills to be able to use technology safely and responsibly. It also incorporates recommendations from KCSIE (September 2021).

The aims of the policy are to ensure that:

3.1. Students, staff, and parents are educated to understand the potential dangers of the internet, mobile phone technology and cyberbullying.

3.2. Knowledge and procedures are in place to prevent incidents of:

3.2.1.misuse of the internet and social media

3.2.2.misuse of email

3.2.3.misuse mobile phones, student devices and related technology

3.2.4.students viewing potentially harmful and inappropriate online material.

4. Scope of the Policy

This policy applies to all members of the Elizabeth College community (including staff, students, volunteers, parents/carers and visitors) who have access to and are users of EC digital technology systems, both in and out of the College.

The Education and Inspections Act 2006 empowers the Principal 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. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered in related policies, Digital Safety and AUP, Anti-Bullying Policy, Student code-of-conduct and Student Disciplinary procedures.

5. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the College:

Directors

The Directors are responsible for the approval of the digital safety policy and for reviewing the effectiveness of the policy. A member of the Board of Directors has taken on the role of Digital Safety Governor. The role of the Digital Safety Governor will include:

5.1. Termly meetings with the DSL, DoDL or the IT Manager.
5.2. Annual attendance at the relevant Digital Strategy Group meetings.
5.3. Termly monitoring of online safety incident logs.
5.4. Reporting to relevant Directors/Board/Committee/meeting

Principal and Senior Leaders

5.5 The Principal has a duty of care for ensuring the safety (including online safety) of members of the college community, though the day to day responsibility for online safety will be delegated to the Digital Safety Team; the Digital Safety Coordinator (DODL) and the DSL (Vice-Principal (Pastoral)).

5.6 The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse”)

5.7 The Principal and Senior Leaders are responsible for ensuring that the Digital Safety Team and other relevant staff receive suitable training to enable them to carry out their digital safety roles and to train other colleagues, as relevant.

5.8 The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in College who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

5.9 The Senior Leadership Team will receive regular monitoring reports from the Digital Safety Team.

Digital Safety Team

The College has an identified Digital Safety Team: DSL (VP (Pastoral)), DODL and IT Manager.

The Digital Safety Team:

5.10 Leads the Digital Strategy Group

5.11 Takes day to day responsibility for digital safety issues and has a leading role in establishing and reviewing the College's digital safety policies/documents.

5.12 Ensures that all staff are aware of the procedures that need to be followed in the event of a digital safety incident taking place.

5.13 Provides training and advice for staff.

5.14 Liaises with College technical staff.

5.15 Receives reports of digital safety incidents and creates a log of incidents to inform future digital safety developments.

5.16 Meets termly to discuss current issues, review incident logs and filtering/change control logs.

5.17 Attends relevant meetings of Directors.

5.18 Reports regularly to Senior Leadership Team.

5.19 Investigates/actions/sanctions with incidents.

Teaching and Support Staff

Are responsible for ensuring that:

They have an up-to-date awareness of digital safety matters and of the current EC Digital safety and AUP.

5.20 They have read, understood, and signed the staff acceptable use agreement (AUP). A summary appears in the staff handbook.

5.21 They report any suspected misuse or problem to the Digital Safety Team for investigation/action/sanction.

5.22 All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.

5.23 Digital safety issues are embedded in all aspects of the curriculum and school activities.

5.24 Students understand and follow the school digital safety and acceptable use policy.

5.25 Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

5.26 They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other college activities (where allowed) and implement current policies with regard to these devices.

5.27 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 Safeguarding Lead (Vice-Principal (Pastoral))

The post holder is trained in online/digital safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

5.28 sharing of personal data.

5.29 access to illegal or inappropriate materials, including terrorist and extremist material which could lead to radicalisation (Prevent Duty).

5.30 inappropriate on-line contact with adults / strangers including potential or actual incidents of grooming.

5.31 Sexting

5.32 cyberbullying

Digital Strategy Group

The Digital Strategy Group provides a consultative group that has wide representation from the college community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. This group is part of the safeguarding group.

Members of the Digital Safety Group will assist the Digital Safety Team with:

5.33 The production/review/monitoring of the College's digital safety policy/documents.

5.34 Mapping and reviewing the digital safety/digital literacy curricular provision – ensuring relevance, breadth, and progression.

5.35 Monitoring network/internet/filtering/incident logs.

5.36 Consulting stakeholders – including parents/carers and the students about the online safety provision.

Students

5.37 Are responsible for using the college digital technology systems in accordance with the student ICT acceptable use agreement.

5.38 Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

5.39 Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

5.40 Will be expected to know and understand policies on the use of mobile devices and digital devices. They should also know and understand college policies on the taking/use of images and on online-bullying.

5.41 Should understand the importance of adopting good online safety practice when using digital technologies out of college and realise that the college's digital safety policy covers their actions out of college, if related to their membership of the college.

Parents/Carers

Parents and 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 and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Parents may underestimate how often young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The college does therefore take every opportunity to help parents understand these issues through:

5.42 parents evenings
5.43 newsletters
5.44 information about digital safety developments.

Parents and carers will be encouraged to support the college in promoting good online safety practice and to follow guidelines on the appropriate use of:

5.45 Digital and video images taken at college events.
5.46 Online Learning Platforms
5.47 Their children's personal devices in the college

Community Users/Guests

Community Users and guests who access college systems as part of the wider college provision will be expected to sign an ICT Acceptable Use agreement before being provided with access to college systems.

6. Policy Statements

Education – Students

The education of students in online safety/digital literacy is an essential part of the College's online safety provision. Young people need the help and support of the College to recognise and avoid online safety risks and build their resilience. Digital safety should be a focus in all areas of the curriculum and staff should reinforce online and digital safety messages across the curriculum. The online and digital safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

6.1 A planned digital safety programme will be provided as part of ICT and PSHE lessons and is regularly revisited. This will cover both the use of ICT and new technologies in school and outside school. At the Upper School this will increasingly be focused upon 'Digital Literacy'.
6.2 Key digital safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.

6.3 Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
6.4 Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
6.5 Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use both within and outside College.
6.6 Rules for use of ICT systems & the internet should be posted in all rooms where computers are accessed.
6.7 It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Support (or other relevant designated person) 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.
6.8 Staff should act as good role models in their use of digital technologies, the internet, and mobile devices.

Education & Training – Staff/Volunteers

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

6.9 A planned programme of formal online and digital safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online and digital safety training needs of all staff will be carried out regularly.
6.10 All new staff should receive online and digital safety training as part of their induction programme, ensuring that they fully understand the college digital safety policy and acceptable use agreements.
6.11 It is expected that some staff will identify online safety as a training need within the performance management process.
6.12 The Digital Safety Team will receive regular updates through attendance at external training events (e.g. from National Online Safety/SWGfL/Black Arrow/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
6.13 Digital safety updates will be presented to and discussed by staff in staff meetings and / or INSET days. The Digital Safety Coordinator will provide advice and guidance to individuals as required.
6.14 This digital safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
6.15 The Digital Safety Team (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Directors

Directors should take part in online and digital safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/ digital safety/health and safety /safeguarding. (Black Arrow to provide – 2022).

Curriculum

Digital safety should be a focus in all areas of the curriculum and staff should reinforce digital safety messages in the use of ICT across the curriculum (see Appendix 4).

6.16 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 follow policies in place for dealing with any unsuitable material that is found in internet searches.

6.17 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should follow the procedure above in Section 6.7

6.18 Students should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.

6.19 Students should not access extremist or terrorist material. Any attempts to do so, should be passed onto the DSL.

6.20 Students should not access socially unacceptable or subversive material. Any attempts to do so, should be passed onto the DSL.

6.21 Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

7. Operational Implementation

Technical – infrastructure/equipment, filtering, and monitoring

The College is 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. The IT Support staff will ensure that systems are kept secure and up to date and will monitor and test the filtering and firewall system, as well as college Email, Teams, BOX and other cloud services.

Elizabeth College employs key technologies to filter and monitor web traffic on our network – transparent filtering and 802.1x BYOD authentication.

7.1 Smoothwall

7.1.1 Smoothwall provides students authenticated device access to the network and filters all traffic from the devices to the internet using Smoothwall's comprehensive and adaptable filtering directory. A daily Smoothwall report is emailed to DSL and DODL to be monitored and reviewed.

7.1.2 Violation procedure:

7.1.2.1 DODL to check daily reports and forward violations to DSL

7.1.2.2 DSL contacts student and parents/guardians and records incident on iSAMS

7.1.2.3 Appropriate information shared with relevant teaching staff

Infrastructure

7.2 College technical systems will be managed in ways that ensure that the college meets recommended technical requirements.

7.3 There will be regular reviews and audits of the safety and security of college technical systems.

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

7.5 All users will have clearly defined access rights to college technical systems and devices.

7.6 All users will be provided with a username and prompted to create a secure password (see password guidance below) by the IT Support team, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

7.7 The College's external network contractors manage the 'super admin' accounts, ensuring that no one person holds these credentials.

7.8 The Colleges' IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

7.9 Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband provider and the college firewall / filtering system (Smoothwall). Content lists are regularly updated automatically and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

7.10 Internet filtering/monitoring should ensure that young people are safe from terrorist and extremist material when accessing the internet.

7.11 College technical staff regularly monitor, and record the activity of users on the college network and users are made aware of this in the acceptable use agreement.

7.12 An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.

7.13 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and individual devices are protected by up to date virus software.

Password Guidance

Staff:

7.14 Staff are required to make a network password consisting of three unrelated words totalling between 12-18 characters. N.B own names are prohibited. Staff will not be prompted to change passwords but MFA is employed to verify by mobile device, new devices or browsers.

Students:

7.15 Students are required to make a network password consisting of three unrelated words totalling between 12-18 characters. N.B own names are prohibited. Students will be prompted to change passwords annually in September.

Anyone who thinks their password may have been compromised must inform the IT Department to inform them of the concern by contacting itsupport@elizabethcollege.gg and also change the password immediately and keep it private.

Mobile Technologies (including BYOD)

Mobile technology devices may be college owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the college's wireless network. All users should understand that the use of mobile technologies should be consistent with and inter-related to other relevant college polices including but not limited to the safeguarding policy, behaviour policy, anti-bullying policy and acceptable use policies.

- The College acceptable use agreements for staff, students and parents/carers will give consideration to the use of mobile technologies:

EC allows:					
	EC owned for single user	**EC owned for multiple user**	**Student owned[1]**	**Staff owned**	**Visitor owned**
Full network Access		*Yes*			
Internet, projectors and printing	*Yes*		*Yes*	*Yes*	
Internet only					*Yes*

[1] Please note that Elizabeth College expects all students to bring a suitable device for use in lessons as per the BYOD policy.

Use of digital and video images

This section should be considered in conjunction with Elizabeth College's Taking, Storing and Using Images of Children Policy available on the website.

7.16 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.

7.17 Staff are allowed to take digital images to support educational aims, but must follow school policies concerning the sharing, distribution, and publication of those images.

7.18 Those images should preferably be taken on school equipment but if staff use their own personal equipment they need to be careful where they store the images taken. It is advised that images are stored on the school storage facility (BOX). An example of this might be a member of staff taking a photo of a student conducting some practical work in Design Technology to upload to their portfolio.

7.19 Care should be taken when taking digital images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

7.20 Students must not take, use, share, publish or distribute images of others without prior permission from the subjects.

8. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection (Bailiwick of Guernsey) Law 2017.

The College must ensure that:

8.1 at all times care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

8.2 personal data is accessed 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.

8.3 the transfer of sensitive data is encrypted and facilitated on secure password protected devices.

8.4 a clear desk policy is followed.

8.5 the reason for sending any sensitive personal data in an email is legitimate and has been considered.

8.6 users only access data while performing their role or that of legitimate professional interest.

9. Communications

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

	Staff and Guests			Students			
Communication Technologies	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the college	X			X			
Use of mobile phones in lessons		X				X	
Use of mobile phones in social time	X					X	
Taking photos on mobile phones/cameras[2]		X				X	
Use of other devices e.g gaming devices							X
Use of BYOD in social time				X[3]			
Use of college email for personal emails			X				X
Using personal devices to take images of students			X				

When using communication technologies, the college considers the following as good practice:

The official college email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the college email service to communicate with others when in college, or on college systems (e.g. by remote access).

9.1 Users must immediately report to the DSL – in accordance with the college policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

9.2 Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These

[2] Students must not take, use, share, publish or distribute images of others without prior permission from the subjects.

[3] BYOD is to be used for curriculum related activities only, misuse will be dealt with in accordance with the sanctions policy.

communications may only take place on official (monitored) college systems. Personal email addresses, text messaging or social media must not be used for these communications.

9.3 Students will be provided with individual college email addresses for educational use.

9.4 Students will be taught about online and digital safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

9.5 Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2021'.
The UK Council for Internet Safety's online Digital Resilience framework reviews how an education establishment protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise.
The College has a duty of care to provide a safe learning environment for students and staff. The College could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the College liable to the injured party.

The College provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the college:

9.6 Ensuring that personal information is not published.

9.7 Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

9.8 Clear reporting guidance, including responsibilities, procedures, and sanctions.

9.9 Risk assessment, including legal risk

College staff should ensure that:

9.10 No reference should be made in social media to students, parents/carers or college staff.

9.11 They do not engage in online discussion on personal matters relating to members of the college community.

9.12 Personal opinions should not be attributed to the college or local authority.

9.13 Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official college social media accounts are established there should be:
A process for approval by senior leaders.

9.14 Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.

9.15 A code of behaviour for users of the accounts, including:

- 9.15.1 Systems for reporting and dealing with abuse and misuse.
- 9.15.2 Understanding of how incidents may be dealt with under college disciplinary procedures.

10. Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from college and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a college context, either because of the age of the users or the nature of those 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/or outside the college when using college equipment or systems. The college policy restricts usage as follows:

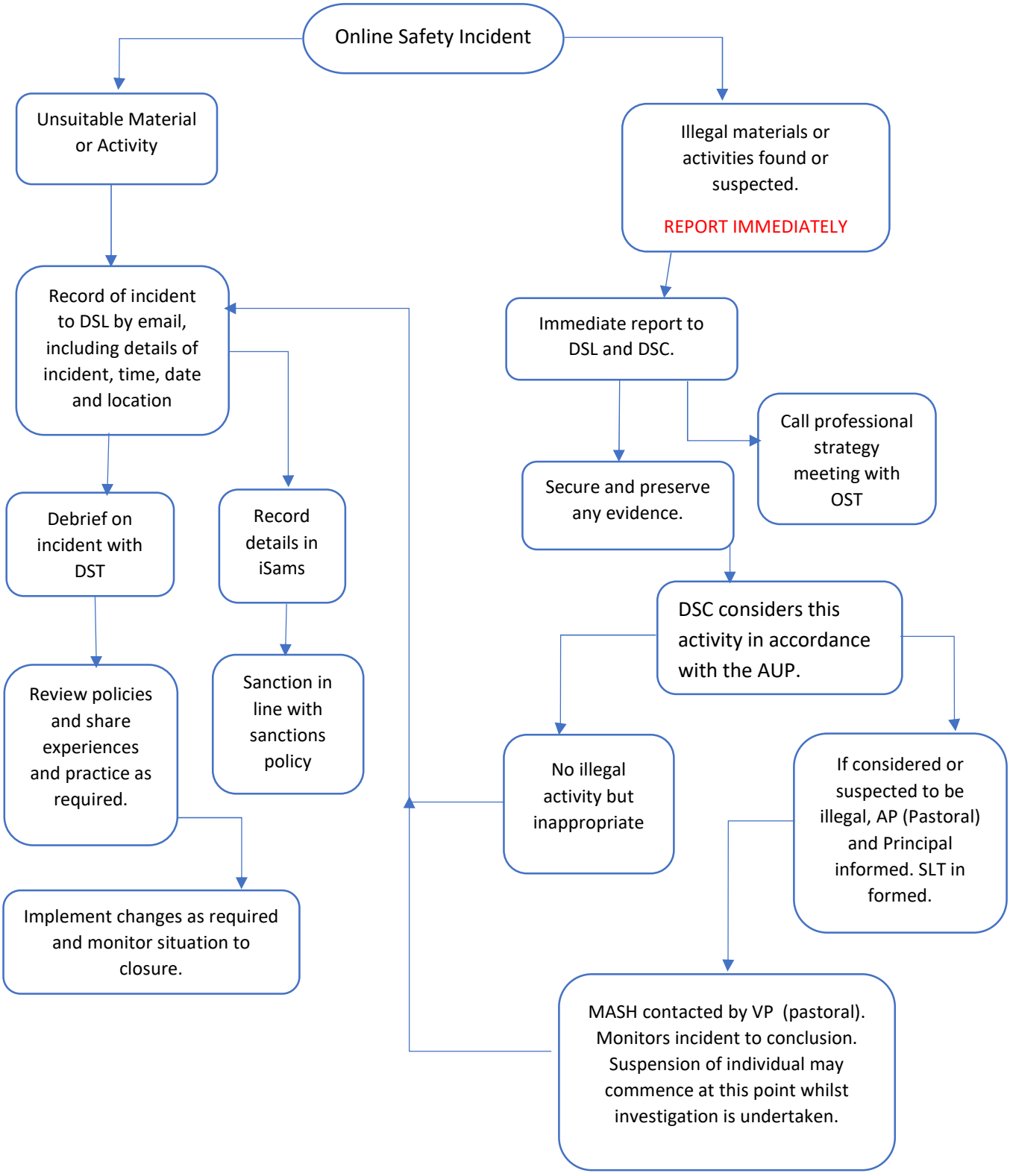
User actions		Acceptable	Acceptable at certain times	Acceptable for certain users	Unacceptable	Unacceptable and Illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008, or Obscene Publications (Bailiwick of Guernsey) Law 1985					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	

	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				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: Gaining unauthorised access to school networks, data and files, through the use of computers/devices. Creating or propagating computer viruses or other harmful files. Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) Disable/Impair/Disrupt network functionality through the use of computers/devices. Using penetration testing equipment (without relevant permission).						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X		
Using college systems to run a private business					X	
Infringing copyright					X	
Online gaming (educational)			X			
Online gaming (non-educational)				X		
Online shopping/commerce			X			
Internal File sharing		X				
Use of appropriate/approved social media		X				
Use of approved messaging apps			X			
Use of video broadcasting e.g. Youtube		X				

Responding to incidents of misuse

It is expected 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, deliberate misuse. This guidance is intended for use when staff need to manage incidents that involve the use of digital services. It encourages a safe and secure approach to the management of the incident; this might involve illegal or inappropriate activities. Below are the responses that will be made to any apparent or actual incidents of misuse: (see “User Actions” above).

Potentially Illegal Incidents



Other incidents

In the event of suspicion, all steps in this procedure should be followed:

10.1 Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

10.2 Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

10.3 It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

10.4 Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

10.5 Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- 10.5.1 Internal response or discipline procedures
- 10.5.2 Involvement by Local Authority or national/local organisation (as relevant).
- 10.5.3 Police involvement and/or action

10.6 If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- 10.6.1 incidents of 'grooming' behaviour
- 10.6.2 the sending of obscene materials to a child
- 10.6.3 adult material which potentially breaches the Obscene Publications Act
- 10.6.4 criminally racist material or promotion of terrorism or extremism
- 10.6.5 offences under the Computer Misuse Act (see User Actions chart above)
- 10.6.6 other criminal conduct, activity or materials

10.7 Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the college and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

11. College action and sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal with in line with Elizabeth College's sanction structure and the Smart Phone and Mobile Devices Policy.

Students Incidents	Refer to class teacher/tutor	Refer to DSL and DSC	Will be referred to SLT	Will be referred to Police/relevant	Refer to IT Support for action re security/filtering etc.	Will be referred to Parents/Carers	General Warning	Further consequence in line with Sanctions	Removal of Network and Internet Rights
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X	X	X		X	
Unauthorised use of non-educational sites during lessons	X	X	X				X	X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X				X	X	
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X	X				X	X	
Unauthorised downloading or uploading of files		X	X		X	X		X	
Allowing others to access college network by sharing username and passwords		X	X		X	X		X	X
Attempting to access or accessing the college network, using another student's account		X	X		X	X		X	X
Attempting to access or accessing the college network, using the account of a member of staff		X	X		X	X		X	X
Corrupting or destroying the data of other users		X	X		X	X		X	X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions		X	X			X	X	X	
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college		X	X			X	X	X	
Using proxy sites, VPNs, or other means to subvert the college's filtering system		X	X		X	X	X	X	
Accidentally accessing offensive or pornographic material.		X	X		X	X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X		X	X
Activity that breaches the Computer Misuse Act.		X	X	X	X	X	X	X	X

Staff Incidents	Refer to line manager	Refer to Principal and HR	Will be referred to SLT	Will be referred to Police/relevant	Refer to IT Support for action re security/filtering etc.	Suspension of Network Account	General Warning	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X	X	X	X	X	X
Inappropriate personal use of the internet/social media/personal email.	X	X	X				X	X
Unauthorised downloading or uploading of files	x	X	X		X			X
Allowing others to access college network by sharing username and passwords	X	X	X		X	X	X	X

Allowing access to the college network by sharing username and password or attempting to access another's network account.	X	X	X		X	X		X
Deliberate actions to breach data protection or network security rules	X	X	X		X	X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X		X		X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students	X	X	X				X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X				X	X
Actions which could compromise the staff member's professional standing	X	X	X				X	X
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college		X	X				X	X
Using proxy sites, VPNs, or other means to subvert the college's filtering system		X	X		X		X	X
Accessing data not relevant to course of performing role or that of legitimate professional interest.	X	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material.		X	X		X		X	
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X		X
Activity that breaches the Computer Misuse Act.		X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X	X

Appendix 1 - Student Acceptable Use Policy

School 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 communication technologies are powerful tools, which open up new opportunities for everyone. Students are expected to bring with them to school an appropriate device (see BYOD specifications) for use in class, this will be used for activities such as research, collaborative learning, promotion of creativity and stimulating awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure…

- that young people will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- 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.

The school will try to ensure that students will have the connectivity to access the digital learning resources required by the curriculum on both Elizabeth College owned devices and personal devices. To ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Consent:

I understand that by logging on to the Elizabeth College wired network or wireless network I am consenting that I have read and agree to abide by the terms set out in the digital safety and Acceptable Use Policy.

Acceptable Use Policy:

I understand that I must use school 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.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line. Personal contact information includes address, telephone numbers, school address and work address.
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

- I will immediately report to a member of staff if I access any offensive or pornographic material whether by mistake or not.
- I will not try to access illegal or inappropriate materials, including terrorist and extremist material which could lead to radicalisation (Prevent Duty).

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. I will not harass or deliberately annoy another person online.
- I will not post information that, if acted upon, could cause damage or a danger of disruption.
- I will not take or distribute images of anyone without their permission.
- I will not knowingly post false or defamatory information about another person or organisation.
- I will not post private information about another person.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand that, when using my own device in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I understand that I will have to download and correctly install the SmoothWall network certificate before I can access the school network.
- I understand that I must not disclose any information to others which would allow or enable access to the College's wireless network. The College accepts no responsibility for any problems that may occur as a result of a portable device being connected to the wireless network.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others as outlined in the Obscene Publications (Bailiwick of Guernsey) Law 1985. I will not try to use any programmes, software or proxy avoidance sites that might allow me to bypass Smoothwall filtering / security systems in place to prevent access to such materials. If I inadvertently access such material, I will immediately report this to a teacher. Elizabeth College reserves the right to confiscate and view devices at any time.

- I will immediately report any damage or faults involving equipment or software, however this may have happened. I will report any possible security problems to IT Support.
- I will not open any attachments to emails, unless I know the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- 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 will not make deliberate attempts to disrupt the Elizabeth College ICT system or to destroy data by spreading a computer virus or by any other means. I am aware that these activities are illegal. Elizabeth College reserves the right to confiscate and view devices at any time.
- I will check my emails frequently, delete unwanted messages promptly and stay within my email quota.
- I will not use chat and social networking sites (or similar) at school.
- I will not access to illegal or inappropriate materials, including terrorist and extremist material which could lead to radicalisation (Prevent Duty). I will report to a member of staff if I have any concerns about other students who try to access such material.
- I will insure that all my communication and interactions are of a positive nature and socially acceptable.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not try to download copies (including music and videos).
- I will not plagiarise work that I find on the internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy, I will be subject to disciplinary action in conjunction with the Behaviour and Rewards Policy. This may include loss of access to the school network / internet, detentions, suspensions, expulsion, contact with parents and in the event of illegal activities involvement of the police.

Appendix 2 - Staff Acceptable Use Policy

School 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.

Consent

I understand that by logging on to the Elizabeth College wired network or wireless network I am consenting that I have read and agree to abide by the terms set out in the digital safety and Acceptable Use Policy.

This Acceptable Use Policy is intended to ensure:

- staff and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy

I understand that I must use school 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 digital 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 communication.
- I understand that the rules set out in this agreement also apply to use of school ICT systems and equipment outside of school.
- I understand that the school ICT systems are primarily intended for educational use.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal or inappropriate use to a member of SLT, the Digital Safety Coordinator or the ICT Manager.

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 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 images. I will not use my personal equipment to store these images.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner. In line with the Safeguarding Policy, I will inform the DSL if I need to use students' personal mobile phone numbers (e.g. for use on school trips or D of E expeditions where remote supervision is appropriate).
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not access or attempt to access any data that is not related to my role or my professional responsibilities or which I have a legitimate professional interest.
- 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, access or circulate any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publication Law (Bailiwick of Guernsey) 1985, or inappropriate material which may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the Smoothwall filtering / security systems in place to prevent access to such materials.
- I will not attempt to access terrorist or extremist material (Prevent Duty).
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, except on my teacher laptop, or store programmes on a computer, nor will I try to alter computer settings.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Policy. Where sensitive personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy 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 Policy Agreement, I could be subject to disciplinary action.

Appendix 3 – Parental Communication

- Parent information evenings in September (Year 8 and Year 10)
- Principal's Letters
- The Week Ahead to include regular updates

Latest advice to parents

Whilst the internet is an amazingly useful tool, we are increasingly concerned about the negative impact that it can also have on young people when used in the wrong manner. It is a topic that we regularly address in College. For this to be effective we encourage parents to work with the College in keeping our children safe online and to use technology in a responsible way. A number of parents have asked for guidance on this topic. If you do want to find out more we recommend the following websites:

Common Sense Media, http://www.commonsensemedia.org/

A US site dedicated to improving the lives of children and families by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology. I would recommend signing up to their weekly newsletters. The site reviews apps, games, music, TV and films to ensure parents are fully informed on the latest releases in all forms of media. It gives age specific recommendations for families.

Get Safe Online http://www.getsafeonline.org/

The UK's leading source of unbiased, factual and easy-to-understand information on online safety. It gives advice on protecting your computer, smartphones and tablets, online shopping, safeguarding children and social networking.

CEOP (Child Exploitation and Online Protection Centre) http://www.thinkuknow.co.uk/

ThinkuKnow is the educational programme of the UK police to keep children safe online and gives age appropriate advice to both parents and children.

Childnet International http://www.childnet.com/

A non-profit organization with the aim of making the internet a great and safe place for children.

Digizen 'Let's Fight it Together' Cyberbullying film (6 minutes)

http://old.digizen.org/cyberbullying/fullfilm.aspx

A film that students at College will watch to help students deal with Cyberbullying.

The South West Grid for Learning (SWGfL) has produced a wide range of information leaflets and teaching resources, including film clips, for students, parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website:

10 Internet Safety Tips - Staying Safe Online | SWGfL

Links to other resource providers:

Internet Watch Foundation (UK Hotline for reporting criminal online content) https://www.iwf.org.uk/
Advice on dealing with Cyber-bullying http://www.cyberbullying.org/
http://www.antibullying.net/cyberbullying1.htm

Safe and Secure Online (advice for parents)

Cyber Safety Resources for Parents (safeandsecureonline.org)

Appendix 4 – Cross Curriculum provision

Detail of curriculum provision is recorded separately in the Wellbeing programme.

Tutors are directed to go through the AUP summary and guidance on dealing with cyber bullying.

Digital Literacy is the term we have given to the development of our Digital Safety provision in Wellbeing. There is an increasing focus on ensuring the boys use the internet effectively and are educated concerning:

- their electronic footprint
- their use of language online
- the effects of bullying
- the effects of violent video games
- the effects of too much time spent online
- over sexualisation of young people due to the effects of pornography, sexting and the media. There will be a particular focus how the internet affects attitudes to relationships.
- Safety online (including the dangers of accessing extremist or terrorist material)

This change of emphasis is important in highlighting the morality angle in the use of the internet.

Appendix 5 - Digital Incident Report Form (Replaced by iSams Module – 2022/23)

(to be completed by the DODL/DSL, monitored by the DSl)

Name of child:		Form group
Nature and detail of incident		
Location		
Action taken: • Parents contacted? • Sanction? • Police involvement? • Communication to school? • Recorded on iSAMS?		
Review of ICT • Improved ICT security		
Signed		**Date**