ELIZABETH COLLEGE

DIGITAL SAFETY 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 pupils with the knowledge and skills to be able to use technology safely and responsibly. This policy is based on the Digital Safety Policy as recommended by the States of Guernsey Digital safety Group (September 2011). It also incorporates recommendations from KCSIE (September 2016) and the Prevent Duty.

1. Aims

The aims of the policy are to ensure that:

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

ii. Knowledge and procedures are in place to prevent incidents of…

- misuse of the internet and social media
- misuse of email
- misuse mobile phones, student devices and related technology
- cyberbullying

2. Scope of the Policy

This policy applies to all members of Elizabeth College, Elizabeth College Junior School (Beechwood and Acorn House) and Guests who have access to and are users of school ICT systems, both in and out of school. If there is an incident of cyber bullying, or other digital safety incident covered by this policy, which may take place out of school, but is linked to membership of the school, the principal can impose disciplinary penalties for inappropriate behaviour where this is reasonable. The College will deal with any incidents in accordance with the Safeguarding Policy and associated behaviour and anti-bullying policies.

3. Roles and Responsibilities

a) The Principal

- is responsible for ensuring the digital safety of members of the school community.
- will appoint a designated person as Digital Safety Coordinator for the school. This will usually be the School's Designated Safeguarding Lead.
- is responsible for ensuring that the Digital Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their safety roles and to train other colleagues, as relevant.

The Principal and another member of the SLT should be aware of the procedures to be followed in the event of a serious digital safety allegation being made against a member of staff.

b) Digital Safety Coordinator: Director of Digital Learning (D Costen)

- takes day-to-day responsibility for digital safety issues and has a leading role in establishing and reviewing the school digital safety policy.
- ensures that all staff are aware of the procedures that need to be followed in the event of an digital safety incident taking place.
- liaises with school ICT technical staff.
- receives reports of digital safety incidents and records them to inform future developments.
- any suspicious online activity of an extremist nature will be reported to www.gov.uk/report-terrorism

They should be trained in digital safety issues and be aware of the potential for serious child protection

issues to arise from:

- sharing of personal data
- access to illegal or inappropriate materials, including terrorist and extremist material which could lead to radicalisation (Prevent Duty)
- inappropriate on-line contact with adults / strangers including potential or actual incidents of grooming
- sexting
- cyberbullying

c) Teaching and Support Staff

All teaching and support staff need to have an up to date awareness of digital safety matters and of the current school digital safety policy and practices & have read and understood the school Staff Acceptable Use Policy (AUP). A summary appears in the staff handbook. Teachers should…

- report any suspected misuse or problem to the Digital Safety Co-ordinator.
- ensure any digital communications with pupils should be on a professional level and only carried out using official school systems.
- ensure digital safety issues are embedded in all aspects of the curriculum and school activities.
- pupils understand and follow the school digital safety and acceptable use policy.
- ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- monitor ICT activity in lessons, extra-curricular and extended school activities.
- be aware of digital safety issues related to the use of mobile phones, cameras and mobile devices. They should monitor their use and implement school policies in regard to their use.
- in lessons they should guide pupils to sites suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

d) Pupils

All pupils are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy. They should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. They also…

- 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 school policies on the use of mobile phones, digital cameras and portable devices. They should also know and understand school policies on the taking and use of images and on cyberbullying.
- should understand the importance of adopting good digital safety practice when using digital technologies out of school and realise that the school's Digital Safety Policy covers their actions out of school, if related to their membership of the school.

e) Parents and 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. The school should therefore take every opportunity to help parents understand these issues through parents evenings, newsletters and information about digital safety developments.

4. Operational Implementation

a) Education (pupils)

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

Digital safety education will be provided in the following ways:

i. A planned digital safety programme should be provided as part of ICT and Wellbeing lessons and should be 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 Ethics'.

ii. Key digital safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.

iii. Pupil should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

iv. Pupils should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices (including Bluetooth) both within and outside school.

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

vi. Rules for use of ICT systems & the internet should be posted in all rooms where computers are accessed.

vii. Staff should act as good role models in their use of ICT, the internet and mobile devices.

b) Education (parents and carers)

Many parents and carers have only a limited understanding of digital safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulating their children's online experiences. Parents often either underestimate or do not realise how often young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through:

- Email communication and the Parent Portal
- Parents evenings

c) Education & Training (Staff)

It is essential that all relevant staff receive digital safety training and understand their responsibilities, as outlined in this policy. Staff will be regularly updated on digital safety developments. It is expected that some staff will identify digital safety as a training need within the professional development process.

All new relevant staff should receive digital safety training as part of their induction programme, ensuring that they fully understand the school digital safety policy and Acceptable Use Policy. 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.

d) 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.

- in lessons where internet use is pre-planned, it is best practice that pupils 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 pupils 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, pupils 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 the temporary removal of 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.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should not access extremist or terrorist material. Any attempts to do so, should be passed onto the DSL.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

e) Use of digital and video images

This section should be considered in conjunction with the Elizabeth College Taking, Storing and Using Images of Children Policy available on the website. When using digital images, staff should inform and educate pupils 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 images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. 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).

Care should be taken when taking digital images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others without appropriate permission.

f) Data Protection

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

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 sensitive data using encryption and secure password protected devices.
- Operate a clear desk policy.
- Consider the legitimate reason for sending any sensitive personal data in an email.
- Only access data in the course of performing role or that of legitimate professional interest.

5. 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, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity for example:

- child sexual abuse images
- material which potentially breaches the Obscene Publications (Bailiwick of Guernsey) Law 1985
- criminally racist material or other criminal conduct, activity or materials

The process outlined below should be consulted and actions followed as indicated.

i. Anyone who suspects inappropriate activity on a school provided computer should:

Report it to the school Digital Safety Coordinator who will make an immediate decision based on what has been reported. Where possible he/she ensures isolation of any involved computer and de-activation of any involved user account.

ii. Digital Safety Coordinator considers this activity in accordance with the AUP.

- **If it isn't considered illegal and isn't considered inappropriate:**
  The incident is closed and details are logged by the Digital Safety Coordinator who ensures account is re-activated and any involved computers returned to use.

- **If it isn't considered illegal but is considered inappropriate:**
  a. The College applies appropriate sanctions.
  b. The College initiates any parallel actions necessary to enhance protection and / or update advice and procedures.
  c. The Digital Safety Coordinator logs details and monitors procedures to closure.

- **If it is considered illegal or if Digital Safety Coordinator is unsure**
  a. The computer is removed or, if a personal device, confiscated and stored securely.
  b. The school Digital Safety Coordinator informs the Principal and AP Pastoral. The SED Serious Incidents Coordinator will then be informed.
  c. The Digital Safety Coordinator logs details and monitors procedures to closure.

- **The SED Serious Incidents Coordinator analyses the evidence from the school**
  a. If an incident is considered to be potentially illegal, the SED Serious Incidents Coordinator contacts the Detective Inspector at the Public Protection Department for advice and /or action.
  b. If an incident is not considered illegal but SED considers further investigation is necessary to enhance protection, SED will instruct ICT / NMS (Network Managed Service) to retrieve information from machine / network.
  c. Logs incident in appropriate file / system.
  d. Monitors procedure to closure.

- **If police advise additional protection measures the Digital safety Co-ordinator initiates action to investigate development and implementation of those measures**

- **The Digital safety Co-ordinator ensures all remedial actions and processes have been put in place and then closes the incident**

a) 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.

b) 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 behaviour / disciplinary procedures.

Appendix 1
Guidance for users at Elizabeth College

Communication at Elizabeth College

Developing communications technologies have the potential to enhance learning and as such all students are expected to have a keyboard-ready mobile device with them for use in lessons. The following list shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages. This list will evolve as technology develops:

i. A suitable (see BYOD Spec) mobile device should be brought to school by all pupils for use in lessons.
ii. Mobile phones and other handheld devices may be brought to school. They may be used in areas outside the 'No Electronic Device' areas during social time but not in lessons unless instructed by the teacher.
iii. Taking photos on mobile phones or other camera devices is not allowed, except with the permission of a teacher for educational purposes.
iv. Use of school email for personal emails is allowed but users should be aware that email can be monitored.
v. Use of chat rooms is not allowed.
vi. Use of social networking sites is not allowed on the school network.

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

i. The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email and message services to communicate with others when in school, or on school systems (e.g. by remote access).
ii. Users need to be aware that email and message service communications may be monitored.
iii. Users must immediately report, to their tutor or Head of Year the receipt of any email or message that makes them feel uncomfortable, they find offensive, threatening or bullying in nature. They should not respond to any such email or message.
iv. Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems.
v. Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
vi. Personal information must not be posted on the school website and only official email addresses should be used to identify members of staff.

Inappropriate activities

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

User Actions

The school is aware of The Obscene Publication (Bailiwick of Guernsey) Law 1985 when making any judgements. 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:

i. Child sexual abuse images
ii. Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation.
iii. Adult material that potentially breaches the Obscene Publications (Bailiwick of Guernsey) Law 1985.
iv. Promotion of any kind of discrimination or racial or religious hatred.
v. Terrorist or extremist material.
vi. Cyberbullying: This is the use of Information and Communications Technology deliberately to upset someone else. It can encompass all areas of the internet, such as email & internet chat room misuse, personal web spaces such as Facebook and threats made by text messaging & the misuse of associated technology, i.e. camera & video facilities. Threatening behaviour may include the promotion of physical violence or mental harm.
vii. Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the school into disrepute.
viii. Using school systems to run a private business.
ix. Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Elizabeth College.
x. Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
xi. Revealing or publicising confidential or proprietary information (e.g. financial, personal information, databases, computer or network access codes and passwords)
xii. Creating or propagating computer viruses or other harmful files.
xiii. 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.
xiv. On-line gaming, gambling, or commerce.
xv. Use of personal social networking sites.

Appendix 2
Examples of misuse and potential sanctions

Deliberate misuse or abuse of the College ICT systems or network will result in sanctions in proportion with the College's behaviour policy. These incidents will include those listed in Appendix 1 and the following:

i. Unauthorised use of non-educational sites during lessons
ii. Unauthorised use of mobile phone / digital camera / other handheld device
iii. Unauthorised use of social networking /instant messaging / personal email
iv. Unauthorised downloading or uploading of files
v. Allowing others to access school network by sharing username and passwords
vi. Attempting to access or accessing the school network, using another pupil's account
vii. Attempting to access or accessing the school network, using the account of a member of staff
viii. Corrupting or destroying the data of other users
ix. Sending an email, text or instant message that is regarded as offensive or of a bullying nature
x. Continued infringements of the above, following previous warnings or sanctions
xi. Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
xii. Using proxy sites or other means to subvert the school's filtering system
xiii. Accidentally accessing offensive or pornographic material and failing to report the incident
xiv. Deliberately accessing or trying to access offensive or pornographic material
xv. Receipt or transmission of material that infringes the copyright of another person or
xvi. Infringes the Data Protection Act

Actions taken in response to misuse:

1. Accounts of those involved maybe disabled.
2. Details of the incident are forwarded to the Head of Year for investigation.
3. The Head of Year investigates the incident matter and reports back to the Administrator and the Digital Safety Coordinator.
4. If misuse has taken place, the Student Account may be disabled for agreed period of time & other appropriate sanctions will be decided, where necessary.
5. More serious offences will be dealt with on an individual basis.
6. Elizabeth College reserves the right to confiscate any device that is deemed to have been used to breach the Digital Safety Policy and AUP.

Appendix 3
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. Pupils 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 pupils 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 pupils 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. I understand that the school will monitor my use of the ICT systems, email and other digital communications.
ii. I will not share my username and password, nor will I try to use any other person's username and password.
iii. I will be aware of "stranger danger", when I am communicating on-line.
iv. 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.
v. I will not arrange to meet people off-line that I have communicated with on-line.
vi. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

vii. I will immediately report to a member of staff if I access any offensive or pornographic material whether by mistake or not.
viii. 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 the 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 pupils who try to access such material.

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. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Appendix 4
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 pupils 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 pupils 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 SMT, the Digital Safety Coordinator or the ICT Manager.

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

a. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
b. I will communicate with others in a professional manner.
c. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
d. 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 record these images, unless I have permission to do so. If these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
e. I will only communicate with pupils 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 pupils' personal mobile phone numbers (e.g. for use on school trips or D of E expeditions or similar).
f. I will not engage in any online activity that may compromise my professional responsibilities.
g. 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.
h. I will not use personal email addresses on the school ICT systems.
i. 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.
j. 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 filtering / security systems in place to prevent access to such materials.
k. I will not attempt to access terrorist or extremist material (Prevent Duty).
l. 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.
m. 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.
n. 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.
o. I understand that data protection policy requires that any staff or pupil 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.
p. 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 5

DIGITAL SAFETY INCIDENT REPORT FORM (if required, often incidents are recorded directly on iSAMS)

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**

Appendix 6
Parent 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 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 pupils at College will watch to help pupils 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 pupils, parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website:
http://www.swgfl.org.uk/staying-safe

Links to other resource providers:

Internet Watch Foundation (UK Hotline for reporting criminal online content)
https://www.iwf.org.uk/

Common Sense Media film clips
http://www.commonsensemedia.org/videos/emmas-story-cyberbullied-by-a-best-friend

Advice on Chat Rooms
http://www.chatdanger.com/

Advice on dealing with Cyber-bullying
http://www.cyberbullying.org/
http://www.antibullying.net/cyberbullying1.htm

Safe and Secure Online (advice for parents)
https://www.isc2cares.org/internet-security-for-kids-parents/

Media Articles
http://www.telegraph.co.uk/education/educationadvice/8593880/Cyberbullying-is-a-new-threat-for-children.html
http://www.telegraph.co.uk/education/educationadvice/10370012/Internet-safety-its-time-to-learn-what-your-children-know.html

Reviewed September 2019
Assistant Principal (Pastoral) and DODL

Appendix 6
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 which is detailed in pupil diaries.

Digital Ethics 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.