Budmouth College

Online Safety Policy

Governors' Committee responsible:	SAC and Personnel
Link Senior Leader responsible:	Jayne Simmonite
Date adopted	29th September 2010
Date reviewed:	March 2017
Next review date:	March 2018

Working Together, Creating Opportunities

This Policy should be read in conjunction with the following Budmouth College policies and documents:

Policies	Documents
Social Media Safeguarding Policy and Child Protection Procedures Code of Conduct Staff Code of Conduct and Guidelines for Safe Working Practices for the Protection of Children and Staff Staff Acceptable Use Policy Student Acceptable Use Policy	Education and Inspections Act 2006 SWGfL Security Policy and Acceptable Usage Policy DCSB Online Safety Information The Children Act 1989 Section 89 of the Education and Inspections Act 2006 Protection from Harassment Act 1997 Criminal Justice and Public Order Act 1994 or Malicious Communications Act 1988 Prevent: Safeguarding Children and Young people against Radicalisation and Violent Extremism

The Policy has been reviewed using the equality impact assessment initial screening record and positive impact is explicitly intended and very likely.

All *policies* can be found on the College 'R' drive in the Policies folder.

Equality Impact Assessment – initial screening record

1. What area of work is being considered?	Online Safety
2. Upon whom will this impact?	All students and staff, volunteers, wider community

3. How would the work impact upon groups; are they included and considered?

The Equality Strands	Negative impact	Positive impact	No impact
Minority ethnic groups		✓	
Gender		✓	
Disability		✓	
Religion, Faith or belief		✓	
Sexual Orientation		✓	
Transgender		✓	
Age (N/A to pre-school and school children)		✓	
Rurality		✓	

4. Does data inform this work, research and/or consultation, and has it been broken down by the equality strands?

	NO	YES	Uncertain
Minority ethnic groups		✓	
Gender		✓	
Disability		✓	
Religion, Faith or belief		✓	
Sexual Orientation		✓	
Transgender		✓	
Age		✓	
Rurality	✓		

Does the initial screening highlight potential issues that may be illegal? ~~YES~~ / NO

Further comments:-

Do you consider that a full Equality Impact Assessment is required? ~~YES~~ / NO

Initial screening carried out by Jayne Simmonite

Signed ……. Date March 17

Comment by Principal: Date…….

Budmouth College Online Safety Policy

This Online Safety policy is based on the SWGfL template. Please see acknowledgements and statement at the end of the policy.

Content

Roles and Responsibilities

Policy Statements

Appendices

Background/Rationale
New technologies have become integral to the lives of young people in today's society, both within College and in their lives outside College. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

However, the use of these new technologies can put young people at risk within and outside the College. Some of the dangers they may face include:

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

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy is used in conjunction with other College Policies such as the Code of Conduct, Use of Social Media Policy and Safeguarding Policy and Child Protection Procedures. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The Online Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy
This Online Safety Policy has been developed, originally, by the Health and Safety Committee composed of:

- College Health and Safety Officer
- Teachers
- Students
- Support Staff
- ICT Technical staff
- Governors

Consultation with the whole College community has taken place through the following:

- Staff meetings
- College Student Council
- INSET Day
- Governors' Strategic Advisory and Personnel Committee (SAC)
- Parents' Evenings
- College website and newsletters

The College will monitor the impact of the Policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity
- Internal monitoring data for network activity
- Surveys and questionnaires of students and parents/carers
- Staff comments and observations

Scope of the Policy

This policy applies to all members of the College community, including staff, students, volunteers, parents/carers, visitors, and community users who have access to and are users of College ICT systems, both in and out of College time.

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 out of College, but is linked to membership of the College. The College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of College.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the College:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the Policy. This will be carried out by the SAC and Personnel Committee receiving regular information about Online Safety incidents and monitoring reports as relevant from the Principal. A member of the Governing Body has the role of Health and Safety Governor. The role of the Health and Safety Governor includes:

- monitoring of Online Safety incident logs
- monitoring of filtering or change control logs
- reporting to the SAC and Personnel Governors' Committee

Principal and Senior Leaders

- The Principal is responsible 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 Student Safety Co-ordinator.
- The Principal through the CPD co-ordinator is responsible for ensuring that the Student Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Student Safety Co-ordinator 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 also support to those colleagues who take on important monitoring roles.
- The Principal and Student Safety Co-ordinator 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 SWGfL flow chart on dealing with Online Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR/disciplinary procedures).

Student Safety Co-ordinator

- Takes day to day responsibility for strategic Online Safety issues and has a leading role in establishing and reviewing the College Online Safety policies and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with College ICT technical staff.
- When relevant, receives reports of Online Safety incidents from the Principal, and creates a log of incidents to inform future Online Safety developments.
- Meets regularly with Link Member of SLT to discuss current issues.
- Reports where necessary to the SAC and Personnel Committee of Governors.

Network Manager/Technical staff

The Network Manager is responsible for ensuring:

- That the College's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the College meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- That users may only access the College's networks through a properly enforced password protection policy.
- SWGfL is informed of issues relating to the filtering applied by the Grid
- That he keeps up to date with Online Safety technical information in order to effectively carry out his Online Safety role and to inform and update others as relevant.
- That the use of the network, including FROG, Citrix and email, is regularly monitored in order that any misuse or attempted misuse can be reported to the Student Safety Co-ordinator.
- That monitoring software/systems are implemented and updated as agreed in College policies.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of the current College Online Safety and social media policies and practices.
- They have read, understood and signed the College Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problem to the Student Safety Co-ordinator for investigation.
- Digital communications with students, such as email, FROG, or voice should be on a professional level and only carried out using official College systems or in line with the Use of Social Media policy.
- Online Safety issues are embedded in all aspects of the curriculum and other College activities.
- Students understand and follow the College Online Safety and Acceptable Use Policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended College activities.
- They are aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current College policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead
The Designated Safeguarding Lead should be trained in Online 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.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Students

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

Parents/Carers
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet or 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 College will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, FROG and information about national and local Online Safety campaigns and literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy.
- Accessing the College website and FROG in accordance with the relevant College Acceptable Use Policy.

Community Users and Visitors
Community Users and visitors who access the College ICT systems, the website, or Frog as part of the Extended College provision will be expected to sign a Community User AUP before being provided with access to College systems.

Policy Statements

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

Online Safety education will be provided in the following ways:

- A planned Online Safety programme should be provided as part of ICT, Citizenship and when appropriate other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College.
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems and the internet are displayed on log-on screens.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education: parents and carers
Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, web site and FROG.
- Parents' evenings.
- Reference to the SWGfL Safe website.

Education: Extended Schools
The College will regularly update parents via Frog on Online Safety issues so that parents and children can together gain a better understanding of these issues. Year 7 parents will be offered the opportunity to attend workshops on this. Messages to the public around Online Safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training: Staff
It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff. An audit of the Online Safety training needs of all staff will be carried out on an annual basis as part of the safeguarding Training programme. It is expected that

some staff will identify Online Safety as a training need within the performance management process.

- All new staff should receive Online Safety training as part of their induction programme and they get Safer Working Practice every 3 years ensuring that they fully understand the College Online Safety Policies and Acceptable Use Policies.
- The Student Safety Co-ordinator will receive regular updates through attendance at training sessions and by reviewing guidance documents released by BECTA/ SWGfL/LA and others.
- This Online Safety & Use of Social Media policies and their updates will be presented to and discussed by staff on INSET days/during meetings.
- The Student Safety Co-ordinator will provide advice, guidance and training as required to individuals as required

Training: Governors

Governors should take part in Online Safety training and awareness sessions, with particular importance for those who are members of the SAC and Personnel Committee. This may be offered in a number of ways:

- Attendance at training provided by relevant organisations.
- Participation in College training and information sessions for staff or parents.
- Technical – infrastructure/equipment, filtering and monitoring.

Technical

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

- College ICT systems will be managed in ways that ensure that the College meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of College ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to College ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Health and Safety Committee.
- All users will be provided with a username and password by the network team who will keep an up to date record of users and their usernames. Staff users will be required to change their password at regular intervals.
- The “master/administrator” passwords for the College ICT system, used by the Network Manager must also be available to the Principal or other nominated senior leader and kept in the College safe.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The College maintains and supports the managed filtering service provided by SWGfL.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

- College ICT technical staff regularly monitor and record the activity of users on the College ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view user's activity.
- Users must report any actual or potential Online Safety incident to either; the Network Manager, Child Protection Officer, Health and Safety Co-ordinator, or more minor incidents to the appropriate behaviour support leader.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the College systems and data.
- Temporary access of "guests" (e.g. trainee teachers, visitors) onto the College system is allowed at the discretion of the Network Manager and Health and Safety Coordinator.
- Executable files may not be downloaded by users without the permission of the Network Manager, and systems are in place to prevent this.
- Personal use may be made of laptops and other portable devices out of College, providing that the personal information of others held on the device is encrypted and password protected.
- Removable media such as memory sticks/CDs/DVDs may be used by users on College workstations or portable devices. However they must not be used to install executable files, or to store personal data unless both the data and the removable media device are protected by password and encryption. In practice this means that most memory sticks will not be suitable for storing personal information relating to others.
- The College infrastructure and individual workstations are to be protected by up to date virus software.
- Personal data may not be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.
- Allocation of digital equipment to a young person.

Curriculum

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

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment

to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet for example on social networking sites.
- Staff re allowed to take digital/video images using to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Those images should **only** be taken on College equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute. Parents/Carers should have given permission for their child to be photographed, normally on the annual contact sheet and this permission recorded on SIMs.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the College website. In most cases this will be on the annual contact form and recorded on SIMs.
- Student's work can only be published with the permission of the student.

Data Protection

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

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

Staff must ensure that they:

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

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

- The data must be encrypted and password protected.
- The device must be password protected: this will exclude many memory sticks/cards and other mobile devices cannot be password protected.
- The device must offer approved virus and malware checking software.

- The data must be securely deleted from the device, in line with College policy (below) once it has been transferred or its use is complete.

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 and disadvantages:

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to 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 or other camera devices owned by the individual rather than the College				x			x	
Use of hand held devices e.g. PDAs, PSPs owned by the individual rather than the College		x					x	
Use of personal email addresses in College, or on College network				x		x		
Use of College email for personal emails	x				x			
Use of chat rooms / facilities (other than FROG)				x				x
Use of instant messaging				x				x
Use of social networking sites				x				x
Use of blogs (this is only allowed if it is a College approved blog for example through Frog)				x			x	

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

- The official College and FROG email service may be regarded as safe and secure and is monitored. Staff should therefore use only the College email service to communicate with students and parents.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the College policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/carers must be professional in tone and content. These communications should only take place on official, monitored, College systems. Personal email addresses, text messaging or

public chat or social networking programmes must not be used for communications with students or their parents.

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

Unsuitable/inappropriate activities

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

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Pornography				**x**
Promotion of any kind of discrimination				**x**
Promotion of racial or religious hatred				**x**
Threatening behaviour, including promotion of physical violence or mental harm				**x**
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute				**x**
Using College systems to run a private business				**x**
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and/or the College				**x**
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				**x**
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				**x**
Creating or propagating computer viruses or other harmful files				**x**
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				**x**
On-line gaming (educational)		**x**		
On-line gaming (non-educational)				**x**

On-line gambling				x
On-line shopping/commerce		x		
File sharing			x	
Use of social networking sites				x
Use of video broadcasting e.g. You Tube		x		

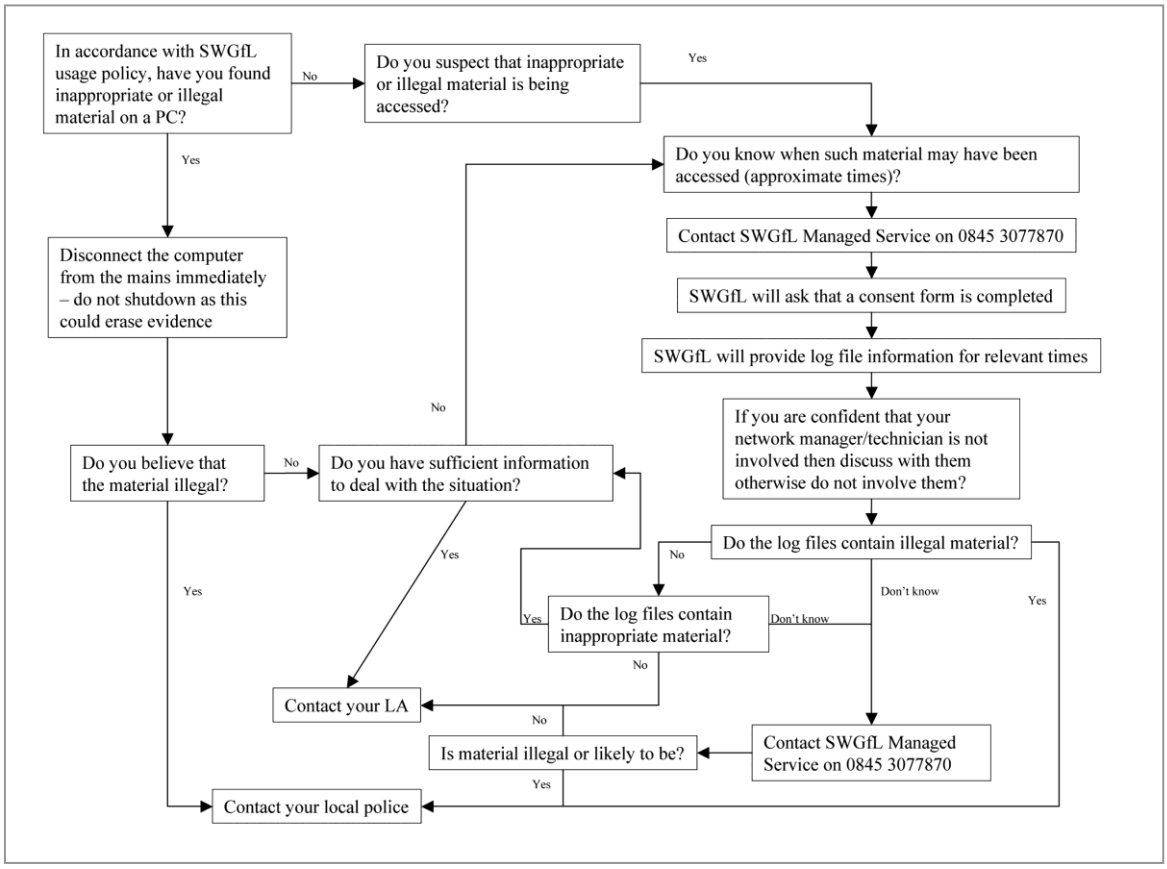
Responding to incidents of misuse

It is hoped that all members of the College community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



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. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security

booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the College 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 College community are aware that incidents have been dealt with. The Principal will decide the appropriate disciplinary sanctions based on the circumstances of the incident.

Further to the flowchart above please ensure that the following actions are completed.

- Take action, record appropriately on the student's file.
- On completion, review actions to see if any organisational procedures need to be changed.

For the victim, consider the following issues:

- Is there further risk of harm?
- Have the parents/carer been informed?
- Should the victim be referred to Social Care as a Child in Need?
- Should a CAF be done to provide support services to the child?
- What are the support needs / vulnerabilities of the child?

If the instigator is also a child:

- Do the Child Protection Procedures apply in respect of the instigator?
- Have the parent/carer be informed?
- Should there be a Risk Assessment of circumstances surrounding the child?
- Should the child be disciplined or provided with guidance/advice/support?
- Should the child's access to technology be monitored /curtailed in the future?

Serious online safety incidents (e.g. Youth Produced Sexual Imagery, grooming, child sexual exploitation, serious threats made or significant risk harm to the victim, or where a person 18 or over is involved) should be referred to the Designated Safeguarding Lead and then referred to the police via the normal **Referrals Procedure**. Incidents that fall within the Dorset Police Youth Internet Safety Policy, i.e. only involve young people under 18 and are not serious may be referred directly from schools to the Safe Schools and Communities Team via the Dorset Police Triage Service.

Online Bullying

Definition

Bullying is behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally. Note that some organisations define bullying as including an imbalance of power. Schools and other agencies will have their own definitions of bullying, which must be communicated to young people, parents and professionals. However, some cases that are one-off incidents, for example friendship issues, may be perceived as bullying by the victim and may therefore need to be dealt with. Online bullying, sometimes referred to as cyber bullying, is bullying that occurs via digital technology, whether that be messenger apps, social media such as Facebook or Instagram or even gaming platforms such as Xbox or PlayStation. It includes but is not limited to:

- Sending threatening or abusive messages;
- Creating and sharing embarrassing images or videos;
- 'Trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games, whether this is from a known or unknown person;
- Excluding someone from online games, activities or friendship groups;
- Setting up hate sites or groups about a particular person;
- Encouraging young people to self-harm;
- Voting for or against someone in an abusive poll;

- Creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

Online bullying has additional issues from offline bullying in that it can happen at all times of the day, there can be a huge audience witnessing the bullying and that it can escalate quickly at the click of a button. Furthermore the content of the bullying can be more unpleasant as perpetrators hide behind the anonymity of the internet. Some online bullying includes prejudice against particular groups, for example on grounds of race, religion, gender, sexual orientation, disability, or because a child is looked after, adopted or has caring responsibilities. Still other online bullying may include threats to harm or kill.

Risks
There are impacts for both victims of bullying and those children and young people who bully. According to Kidscape, children who are bullied are more likely to:

- Have low self-esteem;
- Develop depression or anxiety;
- Become socially withdrawn, isolated and lonely;
- Have lower academic achievements due to avoiding or becoming disengaged with school;
- Be unable to form trusting, healthy relationships with friends or partners in the future.

Children who frequently bully others are more likely to:

- Drop out of, or be expelled from school;
- Engage in criminal behaviour;
- Develop depression or anxiety;
- Be abusive towards their sexual partners, spouses or children as adults.

Bystanders who experience others being bullied may also have feelings of guilt and powerlessness.

Indicators
Young people may report to an adult that they are being bullied online although research suggests that the majority of online bullying is not reported by young people. Online bullying may be reported by a young person's friend or their parents/carers seeing the bullying occurring online. It is not always easy to spot signs of online bullying. However parents/carers and professionals should be alert to changes in behaviour. The following may also be signs of online bullying:

- Being upset after using the internet or their mobile phone;
- Unwilling to talk or secretive about their online activities and mobile phone use;
- Spending much more or much less time texting, gaming or using social media;
- Many new phone numbers, texts or e-mail addresses show up on their mobile phone, laptop or tablet;
- After texting or being online they may seem withdrawn, upset or outraged;
- Not wanting to go to school and/or avoiding meeting friends and school mates;
- Avoiding formerly enjoyable social situations;
- Difficulty sleeping;
- Low self-esteem.

These indicators may also apply to on-line grooming, so practitioners need to vigilant about the range of implications.

Protection and Action to be Taken
Very little online bullying is a police matter. Budmouth's response to online bullying is also covered in the Code of Conduct and the Safeguarding Policy and Child Protection Procedures. This includes recording procedures, including additional procedures required when dealing with incidents involving prejudice against a particular group.

The College has a statutory responsibility to deal with bullying incidents, including online bullying even where it has happened away from the College (Section 89 of the Education and Inspections Act 2006). Where a young person or parent/carer reports to the College that they are being bullied, the College's anti-bullying policy should be used to resolve the situation wherever possible. Where the other parties are within the College, this should be relatively straight-forward to deal with. If the perpetrators of the bullying attend another school and their names and school are known, this information should be passed to the other school to deal with. If the young person is being bullied by an unknown person and this has happened over a period of time, the College may report this to the police. The College will still need to support the victim.

Not all online bullying incidents must be reported to social care or police: while following the relevant procedures, the College should carry out a risk assessment to determine if the incident needs referring to social care and/or the police. Under the Children Act 1989 a bullying incident should be addressed as a safeguarding concern when there is 'reasonable cause to suspect that a child is suffering, or is likely to suffer, significant har.'

The College should provide appropriate advice to the young person and parents/carers including, but not limited to, blocking and deleting people from their contacts list and how to get the content removed from websites using the reporting functions available. Consideration must be given to safeguarding the young person taking into account parents' concerns about use of the device and internet access.

If the material has been reported to the website, game or app via their reporting tools and the material has not been removed, then the College should consider contacting the **Professionals Online Safety Helpline** who may be able to assist. The College should also provide advice to both victims and perpetrators about how to prevent online bullying in future. Practitioners will need to deal with victims, perpetrators and bystanders of this behaviour. Child protection concerns must be referred to Children's Social Care in line with the **Referrals Procedure**.

Where appropriate the incident must be referred to the Police in line with the **Referrals Procedure**: it is generally proportionate to refer any online bullying incidents to the police where the incident could potentially lead to a criminal investigation, for example incidents where threats are made to the victim, incidents involving harassment over a period of time or anything involving hate crimes.

Police Action
There is no specific offence of online bullying. However there a number of existing laws that can be used to prosecute cases of online bullying and harassment, for example Protection from Harassment Act 1997, Criminal Justice and Public Order Act 1994 or Malicious Communications Act 1988 (see Legal Information). It is unlikely that a young person will be prosecuted in relation to online bullying. The current CPS Guidelines on prosecuting cases involving communications sent via social media issued 20 June 2013 state that 'The age and maturity of suspects should be given significant weight [in deciding whether to prosecute], particularly if they are under the age of 18. Children may not appreciate the potential harm and seriousness of their communications and a prosecution is rarely likely to be in the public interest.'

Therefore, not all cases of online bullying involving young people will be investigated. A significant number will be passed to the Safer Schools and Communities Team to liaise with parents/carers and schools to respond under their anti-bullying and behaviour policies.

Youth Produced Sexual Imagery
Please see the Safeguarding Policy and Child Protection Procedures.

Viewing or Uploading Inappropriate Material

Definition

Incidents involving the viewing or uploading of inappropriate material may happen accidentally or deliberately. The types of material that are considered inappropriate include, but are not limited to, images of a sexualised nature featuring adults, material relating to eating disorders or self-harming/suicide, sites encouraging violence and hate, or material that might be capable of radicalising a young person.

Where a person is viewing indecent images of young people under 18 years old or child sexual abuse images these are illegal and will be subject to a criminal investigation.

Where a person is uploading material, it may be that the material may not be illegal or put them at a high risk of abuse, but it may increase their vulnerability to being targeted: for example, uploading a video of themselves to YouTube where they are wearing their Budmouth uniform or taking part in discussions on an inappropriate website.

All regulated online pornography websites try to prevent under 18s from accessing them. The Government has recently clarified existing obscenity laws to ensure that materials rated only suitable for 18 year olds (and above) have controls in place to stop children under 18 from accessing them. There are certain types of pornography that are illegal – even for an adult to be in possession of. These are called "extreme pornographic images", and include acts that threaten a person's life, acts which are likely to, or, result in serious injury, degrading pornography, violent pornography (which includes rape and abuse) or anything involving those under the age of 18. Any images of child abuse are illegal and these should be reported immediately to the **Internet Watch Foundation**, which has responsibility for removing them.

The Pan European Games Information rating system provides guidance as to whether a video game is appropriate or not. The possible age ratings are 3, 7, 12, 16 and 18 and there are further ratings indicating whether the game contains violence, fear, drugs, bad language, sex, discrimination, gambling, and online gaming. These symbols can be found on all games sold in packaging and is now also found on downloadable games from the Google PlayStore, Apple Store etc. In addition, other apps can have ratings defined by the British Board of Film Classification (BBFC).

Risks

There are a number of reasons why young people will access online pornography, including: wishing to learn about sex and sexual identities, curiosity, a want to be sexually aroused, for "a laugh", to break the rules, to be disgusted or to "freak out" their friends (NSPCC).

Research shows that exposure to pornographic content can have significant negative effects on young people including:

- Unrealistic attitudes about sex and consent;
- More negative attitudes towards roles and identities in relationships;
- More casual attitudes towards sex and sexual relationships and increase in 'risky' sexual behaviour;
- Unrealistic expectations of body image and performance.

In relation to inappropriate material that is not related to sexual content, there are still risks associated with viewing and uploading material to these types of sites. There are some sites and online communities where people with anorexia or other eating disorders go to post pictures of themselves and share tips on losing weight. So-called ‘Pro-ana’ websites or 'thinspiration' blogs can be really harmful and negative places as they can encourage people to get dangerously underweight. A young person might believe that these websites are a

good way to talk to people who know what they're going through; however, these sites often make eating problems worse. These sites may also present anorexia or bulimia as a choice rather than a mental illness that can be recovered from. In addition, someone deciding to leave such a site may feel guilty that they are failing to support someone else at risk (Childline). Similar concerns exist in relation to self-harm/injury sites.

Radical and extremist groups may use social networking to attract children and young people into rigid and narrow ideologies that are intolerant of diversity: this is similar to the grooming process and exploits the same vulnerabilities. The groups concerned include those linked to extreme Islamist, or Far Right/Neo Nazi ideologies, Irish Republican and Loyalist paramilitary groups, extremist Animal Rights groups and others who justify political, religious, sexist or racist violence. Children may be drawn to adopt a radical ideology through a failure to appreciate the bias in extremist material; in addition by repeated viewing of extreme content they may come to view it as normal. Young people may self-radicalise by seeking out material themselves or may be groomed in a process similar to that involved in child sexual exploitation.

The risks of online gaming are less clear. Children who play games with PEGI ratings older than their age group may find content that is potentially upsetting. For example, violent or sexualised content or bad language that may be OK for an adult is more likely to upset a young child. Sometimes the viewpoints or behaviour experienced in the games may be copied by children and taken into another environment which can cause risks for other children. Games that can be played over the internet carry the same risks in relation to contacting strangers and conduct risks of bullying or people trying to engage a young person in inappropriate behaviour.

Indicators

A young person or their friends may disclose the content that they have been viewing or uploading or it may be discovered by family, friends or professionals working with the young person or potentially by one of the monitoring strategies a parent/carer may have put in place.

A young person involved with an online community may withdraw from off line communities or family and be focussed heavily on the online community, or they may repeat the views of the online community.

Protection and Action to be Taken

Incidents falling under this category vary greatly in their seriousness and the likely harm to a young person. Practitioners must follow safeguarding procedures in conjunction with these procedures to decide on the most appropriate course of action. Incidents that fall within the Dorset Police Youth Internet Safety Policy, i.e. only involve young people under 18 and are not serious may be referred directly to the Safe Schools and Communities Team: other online safety incidents should be referred to the police via the normal **Referrals Procedure**. Where there are concerns in relation to a child's exposure to extremist materials, procedures around Prevent will be followed (see **Prevent: Safeguarding Children and Young people against Radicalisation and Violent Extremism**). Content of concern can also be reported directly to social media platforms – see **http://www.saferinternet.org.uk/**.

Grooming and Sexual Abuse Using Digital Media

Definition

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation. Children and young people can be groomed online or in the real world, by a stranger or by someone they know - for example a family member, friend or professional. Groomers may be male or female. They could be any age.

Many children and young people don't understand that they have been groomed, or that what has happened is abuse (NSPCC).

When sexual exploitation happens online, young people may be persuaded, or forced, to send or post sexually explicit images of themselves; take part in sexual activities via a webcam or smartphone; or to have sexual conversations by text or online.

Social networking sites or other communications apps are often used by perpetrators as an easy way to access children and young people for sexual abuse. However any website, game or app that allows communication can be used to groom or abuse a young person. Some perpetrators will use the internet to groom one or more young people but their aim is to meet the young person offline for abuse.

The procedures relating to **Organised and Complex Abuse** and **Allegations Against Staff and Volunteers** should be borne in mind depending on the circumstances of the concerns.

Risks
There is some evidence that people found in possession of indecent photographs/pseudo photographs or films/videos of children may now or in the future be involved directly in child abuse themselves. In particular, the individual's access to children should be established to consider the possibility that they are actively involved in the abuse of children including those within the family, within employment contexts or in other settings such as voluntary work with children or other positions of trust. Any indecent, obscene image involving a child has, by its very nature, involved a person, who in creating that image has been party to abusing that child.

Children may be groomed for sexual exploitation on-line.

Indicators
Often these issues come to light through accidental discovery of images on a computer or other device. The initial indicators of abuse are likely to be changes in behaviour and mood of the victim. Clearly such changes can also be attributed to many innocent events in a child's life and cannot be regarded as diagnostic. However changes to a child's circle of friends or a noticeable change in attitude towards the use of computer or phone could have their origin in abusive behaviour. Similarly a change in their friends or not wanting to be alone with a particular person may be a sign that something is upsetting them.

Children often show us rather than tell us that something is upsetting them. There may be many reasons for changes in their behaviour, but if we notice a combination of worrying signs it may be time to call for help or advice.

Issues
When communicating via the internet, young people tend to become less wary and talk about things far more openly than they might when communicating face to face. Both male and female adults and some young people may use the internet to harm children. Some do this by looking at, taking and/or distributing photographs and video images on the internet of children naked, in sexual poses and/or being sexually abused.

Children and young people should be supported to understand that when they use digital technology they should not give out personal information, particularly their name, address or school, mobile phone numbers to anyone they do not know or trust; this particularly includes social networking and online gaming sites. If they have been asked for such information, they should always check with their parent or other trusted adult before providing such details. It is also important that they understand why they must take a parent or trusted adult with them if they meet someone face to face whom they have only previously met on-line.

Children also need to be made aware of the risks involved in sending naked images of themselves to others – Youth Produced Sexual Imagery (sexting).

Allocation of digital equipment to a young person

Advances in internet technology and connectivity have created significant opportunities for children and young people such as access to on-line materials, virtual learning platforms and greater opportunities to communicate and socialise in the virtual world. However we know there are risks and dangers associated with this as described above.

There will be occasions where computers or other digital devices will be issued to children and young people. This protocol has been developed to assist professionals to minimise the risks to the young people, particularly where they will have unsupervised access to the computers (e.g. laptops that they use outside of the organisation).

It is the responsibility of Budmouth to have policies that cover how professionals are expected to work in order to protect young people and themselves where digital technology is used. These should be consistent with this Pan-Dorset online safety policy. Please see Appendix 9 for access to a template letter to be used where digital equipment is to be allocated to a young person.

Prior to issuing digital equipment

- Ensure the hardware has been cleaned and nothing remains on the equipment from the previous user;
- Ensure approved filtering software is installed;
- Inform the Safe Schools and Communities Team (SSCT) who can visit to offer advice and support to the IT Manager on online safety. This includes, if necessary, visiting the young person's home. Tel: 01202 222844 or E-mail: **ssct@dorset.pnn.police.uk**.

On issuing the digital equipment

- Provide up-to-date and age appropriate information to the young person regarding the potential dangers associated with internet use. Useful websites to assist with online safety are given in the Further information section;
- Provide parent/carers with details on how to obtain free software giving guidance on parental monitoring. This can be found via the internet provider;
- Make it clear whether the equipment now permanently belongs to the young person or whether it is on loan and remains the property of your organisation;
- If the equipment remains the property of the College, it would be good practice for an annual check to be carried out regarding how it has been used. If any concerns are raised, advice can be sought from the Safe Schools and Communities Team;
- Anti-malware software will only protect the system if it is up-to-date. Digital equipment therefore needs to be connected to the internet on a weekly basis in order to automatically up-date;
- Encrypted memory sticks containing sensitive information should be stored in a secure manner and never left in the equipment.

Appendices

1. Student Acceptable Usage Policy template
2. Staff and Volunteers Acceptable Usage Policy template
3. Parents/Carers Acceptable Usage Policy Agreement template
4. College Filtering Policy template
5. College Password Security Policy template
6. College Personal Data Policy template
7. College Online Safety Charter
8. Legislation
9. Template letter to be used where digital equipment is to be allocated to a young person.
10. Glossary of terms
11. Further Information
12. Acknowledgements

Appendix 1

Student Acceptable Use Policy Agreement Template
College Policy

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That College ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The College will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use College ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the College will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, 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.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- 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 understand that everyone has equal rights to use technology as a resource and:

- I understand that the College 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 attempt to use the College ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube.)
- 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 take or distribute images of anyone without their permission.

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

- I will only use my personal electronic devices (mobile phones/USB devices etc) in College if I have permission. I understand that, if I do use my own devices in College, I will follow the rules set out in this agreement, in the same way as if I was using College equipment.

- 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, nor will I try to use any programmes or software that might allow me to bypass the filtering/ security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation that sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install or store programmes of any type on any College device nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

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).
- 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 College:

- I understand that the College 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 College and where they involve my membership of the College community (examples would be online bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the College network and internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to College ICT systems.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to College ICT systems.

I have read and understood the above and agree to follow these guidelines when:

- I use the College ICT systems and equipment (both in and out of College)
- I use my own equipment in College (when allowed) e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of College in a way that is related to me being a member of this College e.g. communicating with other members of the College, accessing College email, VLE, website etc.
- I am aware that some online-bullying activities could be classed as a criminal offence.

Name of Student	
Group / Class	

Signed _____ Date _____

Appendix 2

Staff (and Volunteer) Acceptable Use Policy Agreement
College Policy

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the College will monitor my use of College digital technology and communication systems.
- I understand that the rules set out in this agreement also apply to use of College ICT systems (e.g. laptops, email, VLE etc) out of College.
- I understand that the College digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the College.
- 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, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using College 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 College's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the College website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in College in accordance with the College's policies.
- I will only communicate with students and parents/carers using official College systems. Any such communication will be professional in tone and manner

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The College and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the College:

- When I use my mobile devices (laptops/tablets/mobile phones/USB devices etc) in College, I will follow the rules set out in this agreement, in the same way as if I was using College equipment. I will also follow any additional rules set by the College about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the College ICT systems.
- I will not open any hyperlinks in emails or 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 ensure that my data is regularly backed up, in accordance with relevant College policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place to prevent access to such materials.
- Unless I have permission from the network manager I will not 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 network machine, or store programmes on a computer, nor will I try to alter computer settings, other than those allowed through application starter.
- I will not disable or cause any damage to College equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the College Personal Data Policy. Where digital personal data is transferred outside the secure College network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- 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 or by College policy 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 College 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 College:

- I understand that this Acceptable Use Policy applies not only to my work and use of College digital technology equipment in College, but also applies to my use of College systems and equipment off the premises and my use of personal equipment in College or in situations related to my employment by the College.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. In the event of illegal activities this could involve the police.

I have read and understood the above and agree to use the College ICT systems both in and out of College hours and my own devices when in College and/or when carrying out communications related to the College within these guidelines.

Staff/Volunteer Name	
Signed	
Date	

Appendix 3

Parent/Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within Colleges and in their lives outside College. 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. 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 communications technologies for educational, personal and recreational use.
- That College ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their online behaviour. Website for guidance www.thinkuknow.co.uk/parents.

The College will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the **Student Acceptable Use Policy** is on page 3/4 of the Welcome Pack so that parents / carers will be aware of the College expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the College in this important aspect of the College's work.

Permission Form

Parent/Carers Name	
Student Name	

As the parent/carer of the above student, I give permission for my son/daughter to have access to the internet and to ICT systems at College.
I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of College.

I understand that the College will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the College cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
I understand that my son's/daughter's activity on the ICT systems will be monitored and that the College will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the College if I have concerns over my child's Online Safety.

Signed		Date	

Use of Digital/Video Images

The use of digital or video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of College. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the College website and occasionally in the public media.

The College will comply with the Data Protection Act and request parents'/carers' permission before taking images of members of the College. We will also ensure that when images are published that the young people cannot be identified by the use of their full names.

Parents/carers are requested to sign the permission form below to allow the College to take and use images of their children.

Permission Form

Parent / Carers Name	
Student Name	

As the parent/carer of the above student, I agree to the College taking and using digital or video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the College.

I agree that if I take digital or video images at, or of, College events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed		Date	

Appendix 4

College Filtering Policy

Introduction

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

As a part of the South West Grid for Learning (SWGfL) Colleges and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the College's filtering policy will be held by the Network Manager. He will manage the College filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the SWGfL/College filtering service must:

- be logged in change control logs
- be reported to the Health and Safety Co-ordinator:

All users have a responsibility to report immediately to the Network Manager any infringements of the College's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering or security systems in place to prevent access to such materials.

Education, Training and Awareness

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

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

- signing the AUP
- induction training
- staff meetings, briefings, Inset, regular electronic reminders.

Parents will be informed of the College's filtering policy through the Acceptable Use Agreement and through FROG.

Changes to the Filtering System
Users who gain access to, or have knowledge of others being able to access sites which they feel should be filtered or unfiltered should report this in the first instance to the network manager who will decide whether to make College level changes. If it is felt that the site should be filtered or unfiltered at SWGfL level, the Network Manager should email filtering@swgfl.org.uk with the URL.

Monitoring
No filtering system can guarantee 100% protection against access to unsuitable sites. The College will therefore monitor the activities of users on the College network and on College equipment as indicated in the College Online Safety Policy and the Acceptable Use agreement.

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

- the Student Safety Co-ordinator
- SWGfL/Local Authority on request

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

Appendix 5

College Password Security Policy

Introduction

The College will be responsible for ensuring that the College network is as safe and secure as is reasonably possible and that:

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

A safe and secure username and password system is essential if the above is to be established and will apply to all College ICT systems, including email and FROG.

Responsibilities

The management of the password security policy will be the responsibility of the Network Manager. All adults and students will have responsibility for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by a member of the Network Team. Any changes carried out must be notified to the Network Manager. Staff users will change their passwords every term.

Training/Awareness

Members of staff will be made aware of the College's password policy:

- At induction,
- Through the College's Online Safety Policy and Password Security Policy,
- Through the Acceptable Use Agreement.

Students will be made aware of the College's Password Policy:

- In ICT lessons.
- Through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to College ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Personnel and Resources Committee. All users will be provided with a username and password by the Network Team who will keep an up to date record of users and their usernames. Staff users will be required to change their password every term.

The following rules apply to the staff use of passwords:

- Passwords must be changed every term.
- The last four passwords cannot be re-used.
- The password should be a minimum of 8 characters long.
- Must include three of – uppercase character, lowercase character, number, special character.

The following rules apply to all passwords:

- The account should be “locked out” following six successive incorrect log-on attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Requests for password changes should be authenticated by the Network Team to ensure that the new password can only be passed to the genuine user.

The “master/administrator” passwords for the College ICT system, used by the Network Manager must also be available to the Principal and Link SLT VP and kept in the College safe.

Audit/Monitoring/Reporting/Review

The Network Manager will ensure that full records are kept of:

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

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes. User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by the Health and Safety Committee annually. This policy will be regularly reviewed annually in response to changes in guidance and evidence gained from the logs.

Appendix 6

College Personal Data Handling Policy Template

Introduction

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (Becta – Good Practice in information handling in schools – keeping data secure, safe and legal – Sept 2008). It is the responsibility of all members of the College community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- Have permission to access that data.
- Need to have access to that data.

Any loss of personal data can have serious effects for individuals and institutions concerned. It can bring the College into disrepute and may well result in disciplinary action and criminal prosecution. All transfer of data is subject to risk of loss or contamination. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority. The Data Protection Act (1998) lays down a set of rules for processing of personal data. It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Policy Statements

The College will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay. All personal data will be fairly obtained in accordance with the "Fair Processing Code" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The College and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the College community for example names, addresses, contact details, legal guardianship, health and disciplinary records.
- Curricular and academic data, for example class lists, student progress records, reports and references.
- Professional records for example employment history, taxation, national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Responsibilities

Everyone in the College has the responsibility of handling protected or sensitive data in a safe and secure manner. Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The College is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents/Carers – the "Fair Processing Notice"

Under the "Fair Processing" requirements in the Data Protection Act, the College will inform parents/carers of all students of the data they hold on the students, the purposes for which the data is held and the third parties, for example the LA, DCSF, QCA, Ansbury, to whom it may be passed. This fair processing notice will be passed to parents/carers through their child's induction interview and is available on the website. Parents/Carers of young people who are new to the College will be provided with the fair processing notice through their induction interview.

Training & awareness
All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff.
- Staff meetings/briefings/INSET
- Day to day support and guidance from the Student Safety Co-ordinator.

Secure Storage of and access to data
The College will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes. All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on College equipment; this includes computers and portable storage media. Private equipment not owned by the College must not be used. When personal data is stored on any portable computer system, USB stick or any other removable media:

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

The College recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests, namely a written request to see all or a part of the personal data held by the data controller in connection with the data subject.

Data subjects have the right to know if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of College
The College recognises that personal data may be accessed by users out of College, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the College or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of College.
- When data is required by an authorised user from outside the College premises for example, by a teacher working from their home or a contractor they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of data

The College will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

Audit Logging/Reporting/Incident Handling

As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals. The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

The College has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- A "responsible person" for each incident.
- A communications plan, including escalation procedures.
- Results in a plan of action for rapid resolution and
- A plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the Principal to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Appendix 7

Online Safety – A College Charter for Action

Name of School	Budmouth College
Name of Local Authority	Dorset

We are working with staff, students and parents/carers to create a College community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential Online Safety risks.

Our College community

Discusses, monitors and reviews our Online Safety Policy on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years. Supports staff in the use of ICT as an essential tool for enhancing learning and in the embedding of Online Safety across the whole College curriculum. Ensures that students are aware, through Online Safety education, of the potential Online Safety risks associated with the use of ICT and mobile technologies, that all Online Safety concerns will be dealt with sensitively and effectively; that students feel able and safe to report incidents; and that students abide by the College's Online Safety policy.

Provides opportunities for parents/carers to receive Online Safety education and information, to enable them to support their children in developing good Online Safety behaviour. The College will report back to parents/carers regarding Online Safety concerns. Parents/carers in turn work with the College to uphold the Online Safety Policy. Seeks to learn from Online Safety good practice elsewhere and utilises the support of the LA, SWGfL and relevant organisations when appropriate.

Chair of Governors	
Principal	
Student Representative	

Appendix 8

Legislation

The SLT should be aware of the legislative framework under which this Online Safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an Online Safety issue or situation.

The following legislation may apply:

- **Computer Misuse Act 1990** - this Act makes it an offence to:
  Erase or amend data or programs without authority;
  Obtain unauthorised access to a computer;
  "Eavesdrop" on a computer;
  Make unauthorised use of computer time or facilities;
  Maliciously corrupt or erase data or programs;
  Deny access to authorised users.
- **Data Protection Act 1998** - this protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
  Fairly and lawfully processed;
  Processed for limited purposes;
  Adequate, relevant and not excessive;
  Accurate;
  Not kept longer than necessary;
  Processed in accordance with the data subject's rights;
  Secure;
  Not transferred to other countries without adequate protection
- **Freedom of Information Act 2000** - this gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.
- **Communications Act 2003** - sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.
- **Malicious Communications Act 1988** - it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.
- **Regulation of Investigatory Powers Act 2000** - it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
  Establish the facts;
  Ascertain compliance with regulatory or self-regulatory practices or procedures;
  Demonstrate standards, which are or ought to be achieved by persons using the system;
  Investigate or detect unauthorised use of the communications system;
  Prevent or detect crime or in the interests of national security;
  Ensure the effective operation of the system;
  Monitoring but not recording is also permissible in order to:
    - Ascertain whether the communication is business or personal;
    - Protect or support help line staff.

  The College reserves the right to monitor its systems and communications in line with its rights under this act.

- **Trade Marks Act 1994 -** this provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.
- **Copyright, Designs and Patents Act 1988 -** it is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).
- **Telecommunications Act 1984** - it is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.
- **Criminal Justice and Public Order Act 1994** - this defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

  Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.
- **Racial and Religious Hatred Act 2006** - this Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.
- **Protection from Harassment Act 1997** - a person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
- **Public Order Act 1986** - This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.
- **Obscene Publications Act 1959 and 1964** - publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
- **Human Rights Act 1998 -** this does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the College context, human rights to be aware of include:
  The right to a fair trial
  The right to respect for private and family life, home and correspondence
  Freedom of thought, conscience and religion
  Freedom of expression
  Freedom of assembly
  Prohibition of discrimination
  The right to education
  These rights are not absolute. The College is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

- **The Education and Inspections Act 2006** - empowers school Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.
- **Serious Crime Act 2015** - the Act introduces a new offence of sexual communication with a child. This would criminalise an adult who communicates with a child for the purpose of obtaining sexual gratification, where the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16.

Appendix 9

Template letter to be used where digital equipment is to be allocated to a young person.

[DATE]

Dear

Re: ***[name & d.o.b. of child]***

Following discussion, it has been agreed to provide the following special equipment for the above child to use. The equipment will be supplied directly to *[name of organisation or venue].*

Please telephone me when the equipment has been delivered. If the equipment has not been received within 21 days of this letter please contact me.

This equipment is for specific use by the above named child whilst s/he attends your organisation and should be returned to you when the above child no longer attends your organisation or no longer has use for it.

The equipment remains the property of the *[name of organisation]* and all concerned are asked to make every effort to care for the equipment.

Please refer to the Pan Dorset Interagency E-safety procedures which gives advice on all details relating to the equipment and outlines the actions required to ensure the children and young people are kept safe on line.

Arrangements will be made to regularly review this allocation of equipment. Should you have any queries about the loan of this item please do not hesitate to contact me.

Yours sincerely

[Name of provider]

Appendix 10

Glossary of terms

AUP Acceptable Use Policy – see templates earlier in this document
Becta British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
CEOP Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD Continuous Professional Development
CYPS Children and Young Peoples Services (in Local Authorities)
DCSF Department for Children, Colleges and Families
ECM Every Child Matters
FOSI Family Online Safety Institute
HSTF Home Secretary's Task Force on Child Protection on the Internet
ICO Information Commissioners Office
ICT Information and Communications Technology
ICTMark Quality standard for Colleges provided by Becta
INSET In Service Education and Training
IP address The label that identifies each computer to other computers using the IP (internet protocol)
ISP Internet Service Provider
ISPA Internet Service Providers' Association
IWF Internet Watch Foundation
JANET Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
KS1 .. Key Stage 1 (2, 3, 4 or 5) – Colleges are structured within these multiple age groups eg KS3 = years 7 to 9 (age 11 to 14)
LA Local Authority
LAN Local Area Network
Learning Platform A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB Local Safeguarding Children Board
MIS Management Information System
MLE Managed Learning Environment
NEN National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to Colleges across Britain.
Ofcom Office of Communications (Independent communications sector regulator)
Ofsted Office for Standards in Education, Children's Services and Skills
PDA Personal Digital Assistant (handheld device)
PHSE Personal, Health and Social Education
RBC Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for Colleges in England. There are 10 RBCs covering 139 of the 150 local authorities:
SEF Self Evaluation Form – used by Colleges for self-evaluation and reviewed by Ofsted prior to visiting Colleges for an inspection
SRF Self Review Form – a tool used by Colleges to evaluate the quality of their ICT provision and judge their readiness for submission for the ICT Mark
SWGfLSouth West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for Colleges and other organisations in the SW
TUK Think U Know – educational Online Safety programmes for Colleges, young people and parents.
VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP Wireless Application Protocol

Appendix 11

Further Information

General

- UK Safer Internet website
- CEOP website
- ThinkUknow website
- Child Safety Online: A practical guide for parents and carers whose children are using social media

Online bullying

Specialist online bullying organisations include:

- Cybersmile Foundation: Founded in 2010, by the parents of children directly affected by online bullying, the non-profit organisation is committed to tackling all forms of digital abuse and bullying online, by working to promote diversity and inclusion by building a safer, more positive digital community. It also runs 'Stop Online bullying Day' each year in June.
- ChildNet International: Specialist resources for young people to raise awareness of online safety and how to protect themselves.
- The government has produced a number of guidance documents for schools on Preventing Bullying and Bullying at School.

Youth Produced Sexual Imagery

- UKCCIS (2016) 'Youth Produced Sexual Imagery' in schools: advice and support around self-generated images: What to do and how to handle it (March 2013) available from the CEOP website. Responding to Youth Produced Sexual Imagery in schools and colleges – UKCCIS Guidance.
- NSPCC (2012) A qualitative study of children, young people and 'Youth Produced Sexual Imagery'.
- Educational material can be found at http://www.thinkuknow.co.uk/14_plus/need-advice/selfies-and-Youth Produced Sexual Imagery/.
- Viewing and uploading inappropriate material
- Pan European Game Information
- BBFC regulation of mobile content
- BBFC digital age ratings
- UK Safer Internet Bulletin - Protecting Our Children from Radicalisation and Extremism
- NSPCC information about viewing online pornography
- Grooming and sexual abuse using digital media
- Child Exploitation and Online Protection Agency

Appendix 12

Acknowledgements

This policy was developed using the SWGfL framework. SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this College Online Safety Policy Template:

- Members of the SWGfL Online Safety Group and the SWGfL Online Safety Conference Planning Group
- Avon and Somerset Police
- Somerset County Council
- Plymouth City Council
- Swindon Borough Council
- Poole Borough Council
- Bournemouth Borough Council
- North Somerset Council
- Gloucestershire County Council
- DCSF
- Becta
- National Education Network (NEN)
- London Grid for Learning
- Kent County Council
- Northern Grid for Learning
- Bracknell Forest Borough Council
- Byron Review – Children and New Technology – "Safer Children in a Digital World"