COMPASS
NEW DIRECTIONS IN LEARNING
The Compass • 307a Chickerell Road
Weymouth • Dorset • DT4 0QU

Tel: 01305 206530 • Fax: 01305 206531
office@compass.dorset.sch.uk

Compass PRU

E Safety Policy 2017

Governors' Committee responsible	Finance, Resources & Personnel Committee
Link Senior Governor	PFR Committee
Date Reviewed	18/03/17
Next Review Date	March 2018
Linked Policies/Documents	Behaviour Policy Health & Safety Policy Safeguarding Policy Social Media Policy Staff Code of Conduct Student Code of Conduct

Our aim is to help all our learners achieve their full potential in life and work

All policies can be found on the Compass 'R' drive in the Policies Folder

Signed: Alison Glazier — Caroline Peer

Head teacher — Chair of Governors

Date: 21st June 2017 — Date: 21st June 2017

Equality Impact Assessment – initial screening record

	E Safety Policy

1. What area of work is being considered? 2. Upon whom will this impact?	Students, Parents & Staff

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		X	
Gender		X	
Disability		X	
Religion, Faith or Belief		X	
Sexual Orientation		X	
Transgender		X	
Age		X	
Rurality		X	

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

The Equality Strands	No	Yes	Uncertain
Minority ethnic groups		X	
Gender		X	
Disability		X	
Religion, Faith or Belief		X	
Sexual Orientation	X		
Transgender	X		
Age		X	
Rurality	X		

5. Does the initial screening highlight potential issues that may be illegal? **No**

Further comments:-

Do you consider that a full Equality Impact Assessment is required? **No**

Initial screening carried out by

Signed: John Dadds Dated: 6/03/2017

Comment by Headteacher:

Date .....

Compass Learning Centre

E-Safety Policy 2017

Background / Rationale

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

However, the use of these new technologies can put young people at risk within and outside Compass. 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 e-safety policy is used in conjunction with other school policies such as the Behaviour Policy and child protection policies. 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 e-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 e-safety policy has been developed by the e-Safety Co-ordinator in consultation with the Senior leadership Team and staff.

Compass 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' parents / carers
- Staff comments and observations

Scope of the Policy
This policy applies to all members of the Compass community, including staff, students, volunteers, parents/carers, visitors, and community users who have access to and are users of Compass ICT systems, both in and out of school time.
The Education and Inspections Act 2006 empowers the Head Teacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school. Compass 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 e-safety behaviour that take place out of school.

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

Dorset County Council, IT Support fulfils their duties including ensuring the safety of the Compass ICT network.
E-Safety Coordinator for Compass responsible for day to day recording of incidents, maintaining log and staff training.
School Business Manager (DSL) and Assistant Deputy Head Teacher (deputy DSL) are responsible for Safeguarding.
Life Skills teachers are responsible for E-Safety Curriculum.
School Business Manager and Data Manager are responsible for Data Protection in conjunction with DCC IT Services.

Compass Management Committee
Compass Management Committee is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Personnel & Resources Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Health and Safety Governor. The role of the Health and Safety Governor will include:
- meetings with the E- Safety Co-ordinator
- monitoring of e-safety incident logs
- monitoring of filtering or change control logs
- reporting to the Personnel and Resources Governors' committee

Principal and Senior Leaders

 The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the Compass community, though the day to day responsibility for e-safety will be delegated to the E- Safety Co-ordinator.

 The Head Teacher through the CPD co-ordinator is responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

 The E- Safety Co-ordinator will ensure that there is a system in place to allow for monitoring and support of those at Compass who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

 The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

 The Head Teacher and E- Safety Co-ordinator should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures).

E-Safety Co-ordinator

 Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing Compass e-safety policies and documents.
 Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
 Provides training and advice for staff.
 Liaises with the Local Authority.
 Liaises with CEP ICT technical staff.
 Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
 Meets regularly with Head Teacher to discuss current issues, review incident logs and filtering and change control logs.
 Reports where necessary to the Management Committee
 Reports regularly to Senior Leadership Team.

Technical staff

The Technician is responsible for ensuring:
 That Compass's ICT infrastructure is secure and is not open to misuse or malicious attack.
 That Compass meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
 That users may only access Compass's networks through a properly enforced password protection policy.
 SWGfL is informed of issues relating to the filtering applied by the Grid
 That (s)he keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. ??

 That the use of the network, including email, is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator.
 That monitoring software / systems are implemented and updated as agreed in Compass policies.

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

Designated person for child protection / Child Protection Officer
The designated person for child protection should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:
 Sharing of personal data.
 Access to illegal or inappropriate materials.
 Inappropriate on-line contact with adults / strangers.
 Potential or actual incidents of grooming.
 Cyber-bullying.

Students
 Are responsible for using Compass ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to Compass 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 Compass policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Compass policies on the taking and use of images and on cyber-bullying.
 Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that Compass's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet 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. Compass will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local e-safety campaigns and literature.
Parents and carers will be responsible for:
 Endorsing (by signature) the Student Acceptable Use Policy.
 Accessing the Compass website in accordance with the relevant school Acceptable Use Policy.

Community, Users and Visitors
Are responsible for ensuring that:
 They have read, understood and signed the Compass Community, Users and Visitors Acceptable Use Policy (AUP).

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 e-safety is therefore an essential part of Compass's e-safety provision. Children and young people need the help and support of Compass staff to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:
 A planned e-safety programme should be provided as part of Life Skills/Preparation for Working Life and ICT lessons.
 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 Compass.
 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 e-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).
Compass will therefore seek to provide information and awareness to parents and carers through:
 Letters, newsletters, web site.
 Parents' evenings.
 Reference to the SWGfL Safe website.

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

 A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
 All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand Compass e-safety policies and Acceptable Use Policies.
 The E- 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 E-Safety & Use of Social Media policies and their updates will be presented to and discussed by staff in staff meetings and INSET days.
 The E- Safety Co-ordinator will provide advice, guidance and training as required to individuals as required

Training: Management Committee
Members of the Compass Management Committee should take part in e-safety training and awareness sessions, with particular importance for those who are members of the personnel committee. This may be offered in a number of ways:
 Attendance at training provided by relevant organisations.
 Participation in Compass training and information sessions for staff or parents.
 Technical – infrastructure / equipment, filtering and monitoring.

Technical
Compass will be responsible for ensuring that the Compass 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 e-safety responsibilities:

 Compass ICT systems will be managed in ways that ensure that Compass meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
 There will be regular reviews and audits of the safety and security of Compass ICT systems.
 Servers, wireless systems and cabling must be securely located and physical access restricted.
 All users will have clearly defined access rights to Compass ICT systems. Details of the access rights available to groups of users will be recorded by the E-Safety Coordinator and will be reviewed, at least annually.
 All users will be provided with a username and password by the technician and/or E-safety Coordinator 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 Compass ICT system, used by the technician must also be available to the Head Teacher or other nominated senior leader and kept in the Compass 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.
 Compass maintains and supports the managed filtering service provided by SWGfL.

 In the event of the technician 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 E-Safety Co-ordinator.
 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 E-Safety Coordinator or the Head Teacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Co-ordinator
 The Technician regularly monitor and records the activity of users on the Compass 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 e-safety incident to either the Safeguarding Lead or Deputy Officer or E-Safety Co-ordinator.
 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
 Temporary access of "guests" (e.g. trainee teachers, visitors) onto the Compass system is allowed at the discretion of the E- Safety Coordinator in conjunction with the Technician.
 Executable files may not be downloaded by users without the permission of E-Safety Officer and systems are in place to prevent this.
 Personal use may be made of laptops and other portable devices out of school, 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 Compass 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.
 Compass 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 school site unless safely encrypted or otherwise secured.

Curriculum

 E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
 In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
 Where students are allowed to freely search the internet, eg 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the E-Safety Coordinator in conjunction with the Technician, 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 VP, 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. Compass 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 are allowed to take digital / video images to support educational aims, but must follow Compass policies concerning the sharing, distribution and publication of those images. Those images should only be stored on Compass equipment. Personal equipment can only be used to take photographic or video images with prior permission from the Headteacher and can only be stored on a Compass memory card.

 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 Compass 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 school 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 Compass 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 school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students / Pupils			
	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 school, but not used in lessons	x						x	
Use of mobile phones in lessons				x			x	
Use of mobile phones in social time	x				x			
Taking photos on personal cameras using school SD card to store photos (with SLT permission)		x					x	
Taking photos of staff or pupils on personal mobile phones or other mobile devices				x				x
Use of other mobile devices e.g. tablets, gaming devices. (Pupils are allowed to use Compass computers to play age-appropriate games which may be on-line with adult permission and supervision only.)		x					x	
Use of personal email addresses in school, or on school network		x					x	
Use of school email for personal emails				x				x
Use of messaging apps in lessons				x				x
Use of messaging apps in break times	x				x			
Use of social media in lessons				x				x
Use of social media in break times	x				x			
Use of blogs		x				x		

Appendices

Can be found on the following pages:

Unsuitable / inappropriate activities

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

User Actions	Acceptable		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 school 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 (eg 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 eg You tube			x		

Appendices

Can be found on the following pages:

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 E-Safety Charter
8. Legislation
9. Glossary of terms
10. Acknowledgements

Appendix 1

Student Acceptable Use Policy Agreement
Compass 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 Compass ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Compass 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 Compass 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 Compass ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg 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 Compass has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

• I will only use my personal electronic devices (mobile phones / USB devices etc) at Compass if I have permission. I understand that, if I do use my own devices in school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
 I understand 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 attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

 I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

 I will not use chat and social networking sites at Compass

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 Compass:

 I understand that Compass also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the Compass community (examples would be cyber-bullying, use of images or personal information).

 I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Compass 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 Compass 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 Compass ICT systems.

I have read and understand the above and agree to follow these guidelines

- I use the Compass ICT systems and equipment (both in and out of school)

 I use my own equipment in college (when allowed) e.g. mobile phones, PDAs, cameras etc.

 I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the college, accessing Compass email, website etc.

 I am aware that some cyber-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
Compass 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
 That Compass 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.
Compass will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use Compass ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.
For my professional and personal safety:
 I understand that Compass will monitor my use of the ICT systems, email and other digital communications.
 I understand that the rules set out in this agreement also apply to use of Compass ICT systems (eg laptops, email, VLE etc) out of school.
 I understand that the Compass ICT 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 Compass.
 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 Compass 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 Compass'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 (eg on the Compass website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
 I will not use chat and social networking sites on the the Compass ICT network.
 I will only communicate with students and parents / carers using official Compass 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.
Compass and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
 When I use my personal hand held or external devices such as tablets, laptops, mobile phones and USB devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by Compass 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 open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
 I will ensure that my data is regularly backed up, in accordance with relevant Compass 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 except where authorised by the head teacher.
 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 or when authorised by the network manager.
 I will not disable or cause any damage to Compass 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 Compass Personal Data Policy. Where personal data is transferred outside the secure Compass network, it must be encrypted or password protected.
 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 Compass 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. Portable ICT equipment signed out to me for sole use on Compass business is my responsibility to use appropriately and keep safe and secure.
 When using the internet in my professional capacity or for Compass 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 Compass:
 I understand that this Acceptable Use Policy applies not only to my work and use of Compass ICT equipment in Compass, but also applies to my use of Compass ICT systems and equipment out of school time and my use of personal equipment in school or in situations related to my employment by Compass.
 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 understand the above and agree to use Compass ICT systems both in and out of school hours and my own devices when in school and/or when carrying out communications related to Compass 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 school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. 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 Compass 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 e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Compass 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 attached to this permission form, so that parents / carers will be aware of Compass expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of Compass in this important aspect of the school'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 Compass. I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that Compass 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 Compass 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 Compass 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 Compass if I have concerns over my child's e-safety.

Signed

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 Compass. 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 Compass website and occasionally in the public media.

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

Parents are requested to sign the permission form below to allow Compass 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 Compass 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 Compass.

I agree that if I take digital or video images at, or of, Compass 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

Compass 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 Compass has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.
As a part of the South West Grid for Learning (SWGfL) schools 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 Compass's filtering policy will be held by the E-Safety Coordinator in conjunction with the Head Teacher. They will manage the Compass's 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 / Compass filtering service must:
- be logged in change control logs
- be reported to the E-Safety Co-ordinator:

All users have a responsibility to report immediately to the E-Safety Co-ordinator any infringements of Compass'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 e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
Staff users will be made aware of the filtering systems through:
- signing the AUP
- induction training
- staff meetings, briefings, Inset, regular electronic reminders.

Parents will be informed of the college's filtering policy through the Acceptable Use agreement.

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 E-safety Coordinator who will decide whether to make school level changes. If it is felt that the site should be filtered or unfiltered at SWGfL level, the E-Safety Co-ordinator should email filtering@swgfl.org.uk with the URL.

Monitoring

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

Audit / Reporting

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

- the Head Teacher
- 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

Compass Password Security Policy
Introduction
Compass will be responsible for ensuring that the school 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 school's personal data policy.
 Logs are maintained of access by users and of their actions while users of the system

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

Responsibilities
The management of the password security policy will be the responsibility of the Technician and E-safety Coordinator. 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 the Technician or E-Safety Coordinator.

Training / Awareness
Members of staff will be made aware of the Compass's password policy:
 At induction,
 Through Compass's e-safety policy and password security policy,
 Through the Acceptable Use Agreement.

Students will be made aware of the Compass's password policy:
 In ICT lessons.
 Through the Acceptable Use Agreement

Policy Statements
All users will have clearly defined access rights to Compass 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 Management 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 Compass ICT system, used by the Network Manager must also be available to the Head Teacher and kept in the school safe.

Audit / Monitoring / Reporting / Review
The Technician in conjunction with the E-Safety Coordinator will ensure that full records are kept of:
 User IDs and requests for password changes
 User log-ons
 Security incidents related to this policy
 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 Management Committee annually. This policy will be regularly reviewed annually in response to changes in guidance and evidence gained from the logs.

Appendix 6
Compass Personal Data Handling Policy
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 Compass community to take care when handling, using or transferring personal data that it can not 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
Compass 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
Compass 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 Compass 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
Data Protection is the responsibility of the School Manager and Administrator who will keep up to date with current legislation and guidance and will:
 determine and take responsibility for the school's information risk policy and risk assessment.
 appoint the Information Asset Owners (IAOs)

Compass will identify Information Asset Owners (IAOs) for the various types of data being held (eg student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:
 What information is held and for what purpose.

 How information as been amended or added to over time.
 Who has access to protected data and why.

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

Registration
Compass 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, Compass 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, Connexions, 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 Compass 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 Information Asset Owners.

Secure Storage of and access to data
Compass 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 Compass policy (below) once it has been transferred or its use is complete.

Compass 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 Compass
Compass recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:
 Users may not remove or copy sensitive or personal data from Compass 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 (eg family members) when out of school.
 When data is required by an authorised user from outside the school 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
Compass 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.

Compass 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 SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Appendix 7
E-Safety – A Charter for Action
Compass Learning centre
Dorset
We are working with staff, students and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential e-safety risks.

Our school community
Discusses, monitors and reviews our e-safety policy on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years. Supports staff in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole school curriculum. Ensures that students are aware, through e-safety education, of the potential e-safety risks associated with the use of ICT and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that students feel able and safe to report incidents; and that students abide by Compass's e-safety policy.
Provides opportunities for parents/carers to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. Compass will report back to parents / carers regarding e-safety concerns. Parents/carers in turn work with Compass to uphold the e-safety policy. Seeks to learn from e-safety good practice elsewhere and utilises the support of the LA, SWGfL and relevant organisations when appropriate.
Chair of Management Committee
Head Teacher

Appendix 8
Legislation
The SLT should be aware of the legislative framework under which this E-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 e-safety issue or situation.

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
The Freedom of Information Act 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 & 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 Harrassment 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.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

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

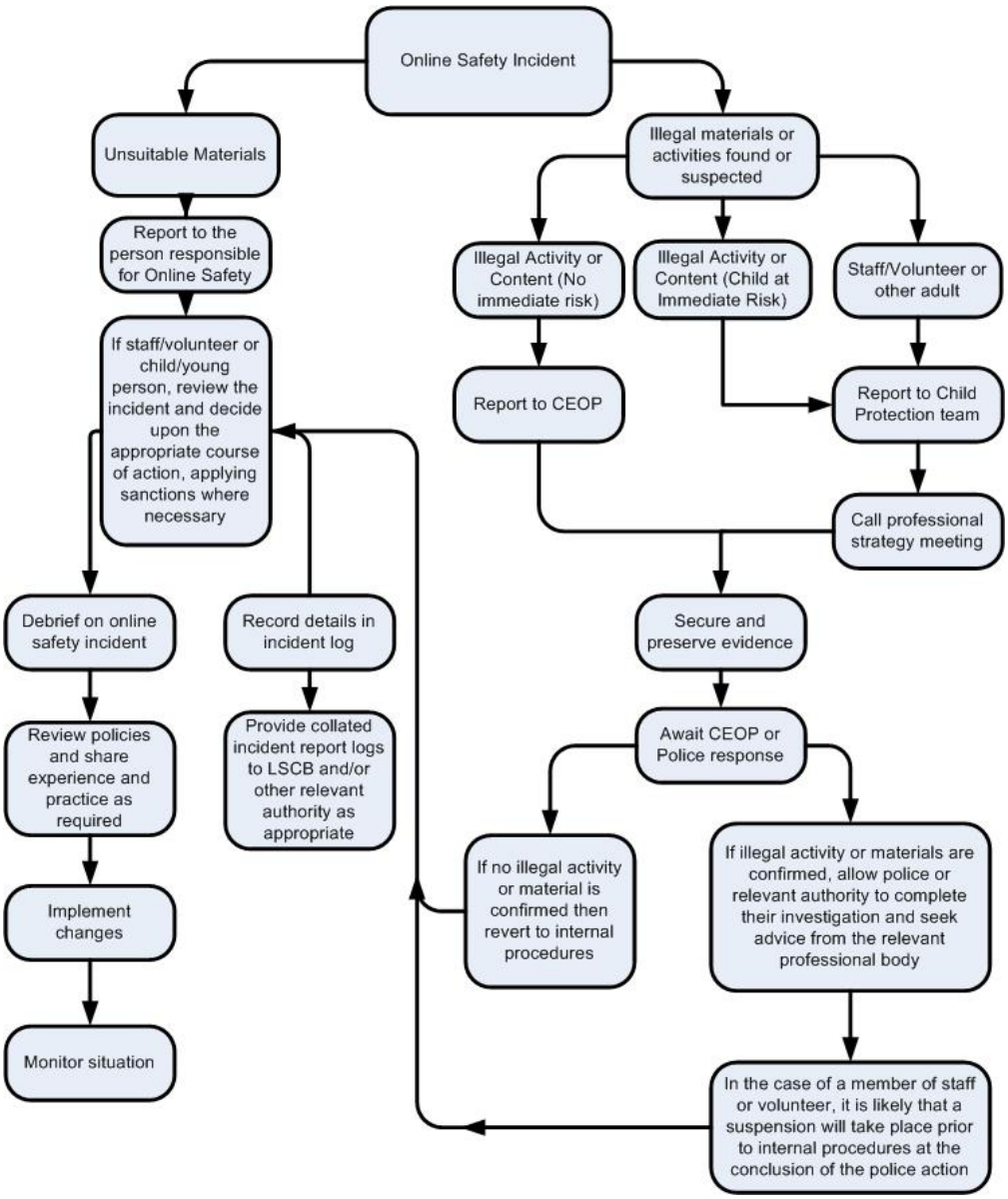
These rights are not absolute. The college is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers 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.

Appendix 9
Responding to incidents of misuse
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). SWGfL BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool)

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

Appendix 10

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 E-Safety Policy Template:

- Members of the SWGfL E-Safety Group and the SWGfL E-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"