EDUCATION
A STATES OF GUERNSEY GOVERNMENT DEPARTMENT

EDUCATION DIVISION
Head of Division: Alan Brown

DOCUMENT TITLE/TOPIC

E-SAFETY POLICY (Schools and Education Services)

DATE OF COMPLETION
July 2010

Ref: No. H&S 26

Status

New	☐
Draft	☐
Policy	☑
Review	☐
Report	☐
Syllabus	☐

PURPOSE:
To provide schools and services with Policy direction on eSafety

RECOMMENDATIONS/ACTION:

WRITTEN BY:
Members of the eSafety Group
Tracey Moore, Group Chairperson

CIRCULATED TO:
Headteachers
Heads of Service
Officers at the Education Department

DATE CIRCULATED:
September 2010

QUERIES TO:
Rob Couch, Head of ICT Services

REVIEW DATE:
September 2011

Contents

Development / Monitoring / Review of this Policy 3
Schedule for Development / Monitoring / Review 3
Scope of the Policy 4
Roles and Responsibilities 4
Headteacher and Senior Leaders: 4
E-Safety Coordinator / Officer: 4
Teaching and Support Staff 5
Students / pupils: 5
Parents / Carers 6
Community Users 6
Operational Implementation 6
Education – students / pupils 6
Education – parents / carers 6
Education & Training – Staff 6
Curriculum 7
Use of digital and video images 7
Data Protection 7
Responding to incidents of misuse 9
E-safety incident process outline 9
Appendices 11
Appendix 1 Guidance for Schools and Education Services 12
Communications 12
Inappropriate activities 13
Appendix 2 Incidents of misuse Actions/Sanctions 15
Appendix 3 Student / Pupil Acceptable Use Policy Template 16
School Policy 16
Acceptable Use Policy 16
Appendix 4 Staff (and Volunteer) Acceptable Use Policy Template 18
Appendix 5 Parent / Carer Acceptable Use Policy Template 21
Use of Digital / Video Images 21
Appendix 6 School Password Security Policy Template 22
Appendix 7 Policy Statements 23
Audit / Monitoring / Reporting / Review 23

Appendix 8 Secondary School Password Policy.....24
Appendix 9 SIMS E-Safety Incident Report Form 29
Appendix 10 Links to other organisations or documents.....31
Appendix 11 Resources.....32
Appendix 12 Glossary of terms.....33

Development / Monitoring / Review of this Policy

This e-safety policy has been developed using The Southwest Grid for Learning template by a working group: Danielle Casselle, Dave Boalch, Ken Wheeler, Linda Armstead, Jane Hunter, Cate Mason, Tracey Moore

Schools will need to agree the content of this document with staff and amend sections where necessary.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by Board	*September 2010*
The implementation of this e-safety policy will be monitored by the:	*Education Forum*
Monitoring will take place at regular intervals:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*September 2011*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*SEN and Children Services Manager and the Head of ICT Service*

The school will monitor the impact of the policy using

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of students / pupils eg CEOP ThinkUknow survey parents / carers staff

Scope of the Policy

This policy applies to all members of States Maintained Schools and Services in the Bailiwick of Guernsey and Elizabeth College and is offered for guidance to all other schools (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Should there be an incident of cyber bullying, or other e-safety incident covered by this policy, which may take place out of school, but is linked to membership of the school, the headteacher can impose disciplinary penalties for inappropriate behaviour where this is reasonable.

The school 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 takes place out of school.

Roles and Responsibilities

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

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher will appoint a designated person as E Safety Coordinator for the school. This will usually be the School's Child Protection Officer.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.
- The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see the incident process outline– included in a later section – "Responding to incidents of misuse").
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

E-Safety Coordinator / Officer:

Each school should have a named member of staff (usually the Child Protection Officer) with a day to day responsibility for e-safety that:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff

- liaises with the SED
- liaises with school ICT technical staff
- receives reports of e-safety incidents and records them on agreed reporting format to inform future e-safety developments, (See Appendix 11 SIMs Logging Sheet)
- reports regularly to Senior Leadership Team

They should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read and understood the school Staff Acceptable Use Policy (AUP) a copy of which is available, displayed in each staff room.
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils 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 school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy,
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school'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 / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school should therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.*

Community Users

Community Users who access school ICT systems / website / VLE should be made aware of the Community User Acceptable Use Policy before being provided with access to the school system.

Operational Implementation

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

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

Education – parents / 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 / 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 school will therefore seek to provide information and awareness to parents and carers through: (select / amend as appropriate)

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

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy:

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

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- All staff will be regularly update with relevant e-safety developments
- This E-Safety policy and its updates *will be presented to and discussed by staff in staff* / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

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 / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where students / pupils 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 the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*
- *Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information*
- *Students / pupils 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

(Make reference to SED Guidance on the Use of Photographic Images of Children)

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school and SED policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without appropriate permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance, including the SED Guidance on the Use of Photographic Images of Children, on the use of such images.
- Students' / Pupils' 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 / pupils are published on the school website
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to Data Protection (Bailiwick of Guernsey) Law 2001

Staff must ensure that they:

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

Responding to incidents of misuse

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

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

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

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

E-safety incident process outline

- **Anyone who suspects inappropriate activity on a School provided computer or on Computer Systems provided by the School / States Education Department :**

  Reports it to school E-safety Coordinator who makes an immediate decision (without actually doing anything on the computer), i.e. can only consider what they can see on screen and what has been reported and where possible ensures isolation of any involved computer and de-activation of any involved user account

- **E-safety Coordinator considers this activity in accordance with the GILE usage policy as amended / published by the school**

  - **If it isn't considered illegal and isn't considered inappropriate:**

    The incident is closed and details are logged on SIMS by E-safety Coordinator who ensures account is re-activated and any involved computers returned to use

  - **If it isn't considered illegal but is considered inappropriate**

    School applies appropriate sanctions and where necessary, contacts parents

    School initiates any parallel actions necessary to enhance protection or update advice / procedures.

    E-safety Coordinator logs details on SIMS and monitors and updates until sanctions / advice / procedures are all completed

    E-safety Coordinator ensures account is re-activated and any involved computers returned to use as appropriate

- **If it is considered illegal or if E-safety Coordinator is unsure**

  Remove the PC and store it securely

  The school E-safety Coordinator informs the SEN and Children's Services Manager and the Head of ICT

  E-safety Coordinator logs details on SIMS and monitors and updates until sanctions / advice / procedures are all completed

  E-safety Coordinator ensures account is re-activated and any involved computers returned to use as appropriate

- **The SED Serious Incidents Coordinator analyses the evidence from the school**

  If an incident is considered to be potentially illegal, the SEN and Children's Services Manager contacts the Detective Inspector at the Public Protection Department for advice and /or action

  If an incident is not considered illegal but SED considers further investigation is necessary to enhance protection, SED will instruct ICT / NMS to retrieve information from machine / network

  Logs incident in appropriate file / system

  Monitors procedure to closure

- **If police advise additional protection measures SEN and Children's Services Manager initiates action to investigate development and implementation of those measures**

- **The SEN and Children's Services Manager ensures all remedial actions / processes have been put in place / followed and closes the incident**

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.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

See Appendix 2 Incidents of Misuse Actions/Sanctions

Appendices

Can be found on the following pages:

Appendix 1	Guidance for Schools and Education Services	11
Appendix 2	Incidents of Misuse Actions/Sanctions	14
Appendix 3	Student / Pupil Acceptable Use Policy Template	15
Appendix 4	Staff (and Volunteer) Acceptable Use Policy Template	17
Appendix 5	Parent / Carer Acceptable Use Policy Template	20
Appendix 6	School Password Security Policy Template	21
Appendix 7	Policy Statements	22
Appendix 8	Secondary School Password Policy	23
Appendix 9	SIMS E-Safety Incident Report Form	28
Appendix 10	Links to other organisations or documents	30
Appendix 11	Resources	31
Appendix 12	Glossary of terms	32

Appendix 1 Guidance for Schools and Education Services

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. This list will evolve as technology develops:

	Staff & other adults				Students / Pupils			
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 school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones or other camera devices								
Use of hand held devices eg PDAs, PSPs								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of chat rooms / facilities								
Use of instant messaging								
Use of social networking sites								
Use of blogs								

The school may also wish to add some policy statements about the use of communications technologies, in place of, or in addition to the above table:

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

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

- Users must immediately report, to the nominated person – in accordance with the school 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 / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1 as required by the school, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Students / pupils 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 school website and only official email addresses should be used to identify members of staff.

Inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, 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 The school should be aware of The Obscene Publication (Bailiwick of Guernsey) Law 1985 when making any judgements. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					☐
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☐
Adult material that potentially breaches the Obscene Publications (Bailiwick of Guernsey) Law 1985					☐
Criminally racist material in UK					☐
Pornography				☐	
Promotion of any kind of discrimination				☐	
Promotion of racial or religious hatred				☐	
Threatening behaviour, including promotion of physical violence or mental harm				☐	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				☐	
Using school systems to run a private business				☐	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by GILE and / or the school				☐	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☐	

Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				☐	
Creating or propagating computer viruses or other harmful files				☐	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☐	
On-line gaming (educational)					
On-line gaming (non educational)					
On-line gambling					
On-line shopping / commerce					
File sharing					
Use of social networking sites					
Use of video broadcasting eg Youtube					

Appendix 2 Incidents of misuse Actions/Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		□	□	□					
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other handheld device									
Unauthorised use of social networking / instant messaging / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another student's / pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or									

infringes the Data Protection Act									

Appendix 3 Student / Pupil Acceptable Use Policy Template

Schools should review and amend the contents of this AUP to ensure that it is consistent with their E-Safety Policy and other relevant school policies. Due to the number of optional statements and the advice / guidance sections included in this template, it is anticipated that the final AUP Agreement will be more concise.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. 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 communication technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

Acceptable Use Policy

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

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will 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 and will immediately report to a member of staff if I access any offensive or pornographic material whether by mistake or not.

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

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

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

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission (schools should amend this section in the light of their mobile phone / hand held devices policies). 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 as outlined in the Obscene Publications (Bailiwick of Guernsey) Law 1985. I will not 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 only use chat and social networking sites with permission and at the times that are allowed (schools should amend this section to take account of their policy on access to social networking and similar sites)

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 school:

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

Appendix 4 Staff (and Volunteer) Acceptable Use Policy Template

It is anticipated that schools will remove the sections which are advisory or for guidance from their final AUP document. Schools should review and amend the contents of this AUP to ensure that it is consistent with their E-Safety Policy and other relevant school policies. Due to the number of optional statements and the advice / guidance sections included in this template, it is anticipated that the final AUP will be more concise.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

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

Acceptable Use Policy

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school. (schools should amend this section in the light of their policies which relate to the use of school systems and equipment out of school)
- I understand that the school 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 the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- 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 school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / 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 school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the Education Department 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 / external devices (PDAs / laptops / mobile phones / USB devices etc) 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 the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (schools should amend this section in the light of their policies which relate to the use of staff devices)
- I will not use personal email addresses on the school ICT systems
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download, access or circulate any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publication Law (Bailiwick of Guernsey) 1985, or inappropriate material which may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, except on my teacher laptop, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school 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 School Policy. Where sensitive personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to the SED and in the event of illegal activities the involvement of the police.

Appendix 5 Parent / Carer Acceptable Use Policy Template

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. 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 school 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.

The school will try to ensure that *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

It is important that parents/carers understand that the school 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. They should understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Parents should understand that their child's activity on the ICT systems will be monitored and that the school will contact them if they have concerns about any possible breaches of the Acceptable Use Policy.

Use of Digital / Video Images

Schools should refer to the SED Guidance on the use of Photographic Images of Children.

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. 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 school website and occasionally in the public media,

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

Appendix 6 School Password Security Policy Template

Introduction

The ICT Section (SED) and NMS will be responsible for ensuring that the *GILE infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the 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 / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy is the responsibility of the Managed Service Provider in collaboration with the ICT section of the SED.

All users (adults and young people) will have responsibility 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.

Requests for passwords for new users, and replacement passwords for existing users can made through the Managed Service helpdesk.

Users will be required to change their passwords every 60 days.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users

Members of staff will be made aware of the SED password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Policy

Pupils / students will be made aware of the SED password policy:

- in ICT and / or e-safety lessons (the school should describe how this will take place)
- through the Acceptable Use Policy

Appendix 7 Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are kept by the Managed Service provider and will be reviewed at least annually, by the ICT section SED.

All users will be provided with a username and password by SED through the Managed Service provider who will keep an up to date record of users and their usernames in an active directory. Staff and secondary pupil users are required to change their password every 60 days.

The following rules apply to the use of passwords: (schools will need to take account of SED guidance and the level of security required factored against the ease of access required for users)

- *staff and secondary pupil passwords are changed every 60 days*
- *the last five passwords cannot be re-used*
- *the password should be a minimum of 8 characters long and*
- *must include one of – uppercase character, lowercase character and number*
- *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 made by the SPOC (Single Point of Contact) with XMA*

Audit / Monitoring / Reporting / Review

Schools should be aware of the States of Guernsey Monitoring Guidance which sets out the legal status of any monitoring activity.

All schools will use the 360 degree safe School E-Safety Self Review Tool. In conjunction with the ICT section the school's current practice will be reviewed in the following areas:

A. Policy and Leadership
B. Infrastructure
C. Education
D. Standards and Inspection

The Managed Service provider will ensure 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.

SED Auditors also have the right of access to passwords for audit investigation purposes

Security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by the ICT Section SED.

This policy will be regularly reviewed (preferably annually) in response to changes in guidance and evidence gained from the logs.

Appendix 8 Secondary School Password Policy

This policy complies with the States of Guernsey Password Policy

1. Policy Statement

The Schools' Information Systems must be protected by passwords to ensure their security. Information Systems must be set up to enforce the requirements of this policy.

2. Purpose

This Policy on the use of passwords is required to prevent unauthorised access to information systems.

3. Scope

This policy applies to all The Schools' systems and employees and students in the Secondary sector.

4. Key Definitions

5. Policy

5.1. User Separation

Unique User IDs must be allocated for each individual user of The Schools' Information Systems. The use of shared passwords or group accounts is prohibited.
User IDs must not be utilised by anyone but the individuals to whom they have been issued.
User IDs should not give any indication of the user's privilege level, (e.g. manager or director). The user's name should be used as the standard User ID, (in the form of initial then surname).

5.2. Responsibility for User IDs

All users of The Schools' information systems, including third parties, are responsible for the activity performed with their personal User IDs, whether or not these User IDs are connecting through external network facilities. User IDs must never be shared with associates, friends, family members, or others.

5.3. User Accountability

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorised user. If users need to share computer resident data, they should use electronic mail, shared folders on local area network servers, or other mechanisms.
Upon login, users must immediately change any default passwords they have been allocated, such as when a new account has been created or when a password has been reset.
Users must immediately change their password if they suspect or know that the password has been disclosed or that a system has been compromised.
Information Technology staff must never ask users to reveal their passwords.

5.4. Choice of Passwords

Passwords need to be obscure in order to minimise the risk of others gaining access.
The current standard for choosing passwords is detailed in the appendix to this document. This defines passwords that should be avoided and gives advice on the selection of passwords. Where possible, systems must be set to re-enforce this standard. This appendix will be updated to represent current best practice.
At the least, user-chosen passwords must be alphanumeric and at least 8 characters in length. Where possible they should use both upper and lower case letters.

5.5. Storage of Passwords

Passwords must not be left in any place where unauthorised persons might discover them.
Information kept with stored passwords must be kept to a minimum.
Paper records of passwords must not be created unless they can be stored safely, i.e. kept in a safe.
Computer files that contain passwords must be password protected and should also be encrypted. It is particularly important that the information in that file is kept to a minimum.
System details, (such as system names and IP addresses), and User IDs should be kept in separate files, which should also be protected.
If any option is given by software for it to remember a password for them, users should decline.

5.6. System Administration
Root passwords must be kept in a fireproof safe and should only be retrieved in an emergency.
When users are provided with their initial password it must be sent in a secure manner and must be valid only for the user's first online session. At that time, the user must be required to choose another password. This same process applies to the resetting of passwords in the event that a user forgets a password.
Sending passwords via email is not secure, as emails are not normally encrypted, so this method must not be used for sending passwords.
Systems must be configured to prevent users from selecting easily-guessed passwords. Please refer to the appendix for advice on allowable passwords.
Where systems permit passwords must be set to expire after a maximum period of up **to 60 days.**
Users must be prevented from reusing previous passwords. System owners should record those staff with static passwords (but not the passwords themselves)
All vendor-supplied default fixed passwords must be changed before any computer or communications system is used for The Schools' business.
The display and printing of fixed passwords must be masked, suppressed or otherwise obscured such that unauthorised parties will not be able to observe or subsequently recover them.
The number of consecutive attempts to enter an incorrect password must be strictly limited. After up to five unsuccessful attempts to enter a password, the involved user ID must be suspended until reset by a system administrator or temporarily disabled for no less than three minutes. Where network connections are involved, the session must be disconnected or a time-out period must be initiated.

5.7. Password Compromise
Whenever system security has been compromised or if there is a reason to believe that it has been compromised, the involved system administrator must immediately change all involved privileged user passwords and require every end-user password on the involved system to be changed at the time of the next log on. If systems software does not provide the latter capability, a broadcast message must be sent to all users telling them to change their passwords immediately.

6. Supporting Documents
The Information and Communications Technology Security Policy, published by the Information Technology Unit, defines this policy.
Users agree to comply with the provisions of this policy upon signing the Acceptable Use Declaration attached to the ICT Acceptable Use Directive.

7. Administration
This policy can be found on The Schools' Website at http:
This policy will be reviewed every three years by the Security Working Group.
The IT Unit, and/or the appropriate local IT section, will keep a record of authorised users and administrators.

8. Interpretation
If there are any questions about this policy, please phone
Users are to await a formal response from the IT Unit, or their local IT section, before carrying out any action that they are unsure about.

9. Monitoring
Information about incidents may be collected for trend/statistical purposes or for reference to solve similar incidents in the future.
Subject to relevant legislation, The Schools reserve the right to monitor, regulate and audit any data stored on or crossing through any The Schools' information systems. Communications may be confidentially audited and monitored, in accordance with legislation, to protect the departments and The Schools and to ensure that guidelines are being followed.
By making use of The Schools' systems, users consent to permit all information stored on or crossing through The Schools' systems to be monitored, regulated, audited or divulged to law enforcement at the discretion of Senior Officers. Users not involved in this process must not intercept, disclose or assist in intercepting or disclosing any electronic communications.
10. Violations and Enforcement
Any violations of any policy issued by The Schools must be reported to the IT system providers, to an appropriate IT support section Manager or to your local HR representative.
The response to any incident must follow the IT Incident Management Procedures.
Any investigation into alleged misconduct must follow the appropriate staff directive on discipline.
Any breach of policy in the use of The Schools' equipment may be considered as grounds for disciplinary action. Any illegal or criminal activity will be passed to law enforcement.

11. Compliance
This policy intends to meet legal and regulatory compliance including, but not limited to:
The Data Protection (Bailiwick of Guernsey) Law 2001
The European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Guernsey) Ordinance, 2004
The Regulation of Investigatory Powers (Bailiwick of Guernsey) Law 2003
The Computer Misuse (Bailiwick of Guernsey) Law 1991
The Wireless Telegraphy (Channel Islands) Order 1952
The International Standard 27002: Code of practice for information security management.

12. References
ISO27002:2005 11.2.3 – User Password Management
ISO27002:2005 11.3.1 – Password Use
ISO27002:2005 11.5.2 – User Identification and Authentication
ISO27002:2005 11.5.3 – Password Management System

13. Appendix: Password Selection

13.1. Passwords to Avoid

A match can be found for any password on any system eventually. Tools are available to quickly try every name and every word in a dictionary. This is called a 'dictionary attack'. Dictionary attack tools can try around 1 million passwords per second.

Passwords should not:

- Be any dictionary word or a name.

- Be related to a user's job or personal life, unless accompanied by additional unrelated characters. For example, a car license plate number, a spouse's name or fragments of an address.

- Be identical or similar to passwords they have previously employed.

- Contain consecutive identical characters.

- Contain common character sequences, such as ‘123456’

- Be a derivative of the User ID.

- Be constructed using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must not employ passwords like "X34JAN" in January and "X34FEB" in February.

13.2. Tips on Choosing Strong Passwords

Users can choose easily-remembered passwords that are difficult for unauthorised parties to guess if they:

- String together several words into a pass phrase. Or base the password on the first letters of each word in a pass phrase.

- Shift a word up, down, left, or right one row on the keyboard.

- Bump characters in a word a certain number of letters up or down the alphabet.

- Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word.

- Combine punctuation, numbers or special characters (‘@£%&’ etc) with a regular word.

- Deliberately misspell a word.

Good ideas

cvc#cvc# is a technique that can be used to make obscure passwords that stick in your mind. In this technique passwords use a random consonant followed by a random vowel then another consonant. The hash (‘#’) represents a number or special character. This process is repeated for the second half of the password. For example: ‘boz5tud2’, ‘wof9reh1’ etc. Another technique is to break up a password by inserting special characters between each letter in the password: for example, p # a % s £ s * w (o @ r / d.

14. Appendix: Grammar School ideas from Val Francis

Proposed password security protocol/process

1) Secure unique passwords:

Should include at least one upper case letter

Should be a combination of letters and numbers

Should not be proper words or names (random in their nature)

Users should not be allowed to use rapid change passwords
No use of repeat passwords within 5 password changes
Should Force a change of password every 60 days

2) Management of passwords

Should allow access for individual in school to manage password allocation and deal with any issues relating to forgotten passwords and mistyped passwords

3) Managing passwords with younger/less able children

Not applicable for our cohort

4) How we move/educate children towards the need and management of secure passwords

It is envisaged that this should be addressed during induction process in Year 7 ICT classes. Change of protocol in short term- managed through ICT classes and should also include attempt to embed reasons for and principles of password discipline to all students (applicable to all areas of online interaction and security).

5) The process required to roll out passwords to children.

This should be managed in schools as part of ICT lessons/ e-learning induction/ Personal development programme (post 16). It will be necessary to make very link clear between e-safety and password discipline.

Schools are given a clear rationale for increased security and deadline for when technical changes will be enforced. By this time, it would be expected that staff & students have adapted to new set of expectations, and taken afore mentioned steps to improve levels of password security.

School	AMHERST PRIMARY SCHOOL
Date and Time:	17 June 2010 In School Hours
Nature of Incident:	E-Safety Pupil
Type of Incident:	ES - Defamatory Content
Description of Incident:	
Location:	ES - School Network School Device
Status:	Help Required

Appendix 9 SIMS E-Safety Incident Report Form

E-SAFETY INCIDENT REPORT FORM

To be completed before sending to the Department	
Has this child been involved n a similar incident before? Outline the support given for the Child How many other incidents of this type have occurred this half term?	

Signed.....E Safety Co-ordinator
Date.....

Name	Date	Time	Type	Activity	Location	Comment
Dannielle Allen	17 June 2010	In School Hours	E-Safety Pupil	ES - Defamatory Content	ES - School Network School Device	

Outcome	Status	Parents Informed	Action Taken	Staff Involved
Removal of Internet Access	Help Required	Yes	Removal of Internet Access	

Appendix 10 Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

SOUTH WEST GRID FOR LEARNING:
"SWGfL Safe" - **http://www.swgfl.org.uk/safety/default.asp**

Child Exploitation and Online Protection Centre (CEOP)
http://www.ceop.gov.uk/

ThinkUKnow
http://www.thinkuknow.co.uk/

CHILDNET
http://www.childnet-int.org/

INSAFE
http://www.saferinternet.org/ww/en/pub/insafe/index.htm

BYRON REVIEW ("Safer Children in a Digital World")
http://www.dcsf.gov.uk/byronreview/

Becta
Website e-safety section - **http://schools.becta.org.uk/index.php?section=is**
Developing whole school policies to support effective practice:
http://publications.becta.org.uk/display.cfm?resID=25934&page=1835
Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:
http://publications.becta.org.uk/display.cfm?resID=32422&page=1835
"Safeguarding Children in a Digital World"
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

LONDON GRID FOR LEARNING
http://cms.lgfl.net/web/lgfl/365

KENT NGfL
http://www.kented.org.uk/ngfl/ict/safety.htm

NORTHERN GRID
http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp

NATIONAL EDUCATION NETWORK
NEN E-Safety Audit Tool: **http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html**

CYBER-BULLYING
DCSF - Cyberbullying guidance
http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007
Teachernet
http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/
Teachernet "Safe to Learn – embedding anti-bullying work in schools"
http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/
Anti-Bullying Network - **http://www.antibullying.net/cyberbullying1.htm**
Cyberbullying.org - **http://www.cyberbullying.org/**

Appendix 11 Resources

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website:

http://www.swgfl.org.uk/safety/safetyresources.asp?page=schoolst_resources&audienceid=3

Links to other resource providers:

BBC Chatguides: **http://www.bbc.co.uk/chatguide/index.shtml**

Kidsmart: **http://www.kidsmart.org.uk/default.aspx**

Know It All - **http://www.childnet-int.org/kia/**

Cybersmart - **http://www.cybersmartcurriculum.org/home/**

NCH - **http://www.stoptextbully.com/**

Chatdanger - **http://www.chatdanger.com/**

Internet Watch Foundation: **http://www.iwf.org.uk/media/literature.htm**

Digizen – cyber-bullying films: **http://www.digizen.org/cyberbullying/film.aspx**

London Grid for Learning: **http://cms.lgfl.net/web/lgfl/safety/resources**

Appendix 12 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, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
GILE	Guernsey Interactive Learning Environment
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools 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) – schools are structured within these multiple age groups eg KS3 = years 7 to 9 (age 11 to
LAN	Local Area Network
Learning	A learning platform brings together hardware, software and supporting services
Platform	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 schools across Britain.
NMS	Network Managed Service

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 schools in England. There are 10 RBCs covering 139 of the 150 local authorities.
SED	States Education Department
SEF	Self Evaluation Form – used by schools for self evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, 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