Kinlochleven High School

E-Safety Policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group / committee made up of:

- The Head teacher / Principal / Senior Leaders
- E-Safety Officer / Coordinator
- Child Protection Coordinator
- Staff, including teachers, support staff and technical staff
- Parents and Carers/Parent Council representation
- Community users

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was agreed	*Insert date*
The implementation of this e-safety policy will be monitored by the:	*E-Safety Coordinator* *E-Safety Committee,* *Senior Management*
Monitoring will take place at regular intervals:	*Insert time period (suggested to be at least once a year*
The *Headteacher/Senior Leadership Team* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Insert time period (suggested to be at least once a year*
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:	*Insert date*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Area Lead Officers (Care and Learning)* *Police*

The school will monitor the impact of the policy using:

- *logs of reported incidents;*
- *monitoring logs of internet activity (including sites visited);*
- *Surveys / questionnaires of:*
    - *children/young people;*
    - parents / carers;
    - *staff.*

Scope of the Policy

This policy applies to all members of the school community (including staff, children / young people, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school

Schools need to be aware that incidents of cyber-bullying, or other e-safety incidents covered by this policy may take place outside of the school, between children and young people who attend the school or between any members of the school community, including staff. The school and the education authority, in partnership with parents needs to decide how to deal with such incidents and make this clear in the policy. This will link closely with positive relationships and behaviour policy and anti-bullying policies. The policy should make clear how the school will involve parents in relation to such incidents.

Roles and Responsibilities

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

Education Authority

Schools should work very closely in partnership with officers from their authority to ensure that their school policies and procedures are in line with local and national advice and inter-agency approaches to the care and wellbeing of children and young people.

Headteacher / Principal and Senior Leaders:

- T**he *Headteacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator / Officer.*
- T**he Headteacher and (at least) another member of the Senior Membership 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 flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Education Authority HR / other relevant body* disciplinary procedures).
- *The Headteacher / Principal / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*
- *The Headteacher / Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school 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 Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer*

E-Safety Coordinator:

The E-Safety Coordinator has a day to day responsibility for e-safety and will refer incidents regarding Child Protection to senior management.

- leads the e-safety group;
- 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 Education Authority / relevant body;

- liaises with school technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with relevant officer from Education Authority to discuss current issues, review incident logs and filtering / change control logs. This may be officer responsible for supporting schools in relation to Child Protection or network manager/officer supporting ICT infrastructure;
- attends relevant meetings of pastoral care team and/or senior leadership team;
- reports regularly to Senior Leadership Team.

Designated Getting it right for every child - Named Persons:

Getting it right for every child (GIRFEC) is the national policy aimed at improving outcomes for all children and young people. It provides the overarching approach to support delivery of all other policies for children, young people and families. The *Getting it right* approach includes a *Named Person* for every child, from birth (or sometimes before), until they reach 18. The Named Person will record and action any concern about a child's wellbeing that has come to their attention, either through their own knowledge of the child or if a concern is raised by another service or from within their own organisation.

The **Named Person** – will promote, support and protect a child or young persons wellbeing, will be the first point of contact for the child and their family – will take action, help, or arrange for the right help in order to promote the child's development and wellbeing. The Named Person will, due to their role, have an oversight of known issues in the child's life and will be able to use that oversight, in collaboration with other services, to make a professional judgement on the most appropriate and proportionate course of action.

Named Persons **- In education** the designated Named Person will be a promoted member of staff within the school, usually the head teacher. In practice the role of the Named Person may be delegated to be carried out by an appropriate promoted or specialist teacher. The Named Person will be part of a network of support and will themselves be supported by the management framework and procedures in place within the local authority and partnerships. The Named Person will record and action any concern about a child's wellbeing that has come to their attention, either through their own knowledge of the child or if a concern is raised by another service or from within their own organisation. Named Persons will have access to and be required to manage and store personal and sensitive information, as such they will be acutely aware of the practices and procedures in respect of e-security

Network Manager :

Kinlochleven High School has a managed ICT service provided by an outside contractor WIPRO, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below.

WIPRO is responsible for ensuring:

- **that the school technical infrastructure is secure and is not open to misuse or malicious attack;**

- **that the school meets required e-safety technical requirements and any *Local Authority / other***
- ***relevant body* E-Safety Policy / Guidance that may apply;**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;**
- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep 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 / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher / Principal / Senior Leader ; E-Safety Coordinator* for investigation and action;
- *that monitoring software / systems are implemented and updated as agreed in school / academy 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 school e-safety policy and practices;**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP);**
- **they report any suspected misuse or problem to the *Headteacher / Principal / Senior Leader ; E-Safety Coordinator* for investigation and action;**
- **all digital communications with children/young people / parents / carers 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 activities;
- children / young people understand and follow the e-safety and acceptable use policies;
- children / young people have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- teachers monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- *in lessons where internet use is pre-planned children/young people 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.*

Child Protection Coordinator

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;
- Inappropriate sharing of images, for example through mobile phones.

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring of the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the *headteacher / senior leadership team/Pupil Support team.*

Members of the *E-safety group* will assist the *E-Safety Coordinator* with:

- the production / review / monitoring of the school e-safety policy / documents;
- *the production / review / monitoring of the school filtering policy will be conducted by WIPRO*
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression;
- monitoring network / internet / incident logs;

- consulting stakeholders – including parents / carers and the children / young people about the e-safety provision;
- monitoring improvement actions identified through use of the 360 degree safe self review tool.

Children / young people:

- **are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy for children/young people;**
- 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. They need to **un**derstand the need to protect themselves and respect others when participating in social networks;
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand 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;
- should demonstrate an understanding of digital citizenship and how it links to their roles and responsibilities within 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. The school will take every opportunity to work closely in partnership with parents on these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website / VLE and on-line student / pupil records;
- their children's personal devices in the school (where this is allowed).

Community Users

Community Users who access school systems / website / VLE as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Children / Young People

Whilst regulation and technical solutions are very important, their use must be balanced by educating *children / young people* to take a responsible approach. The education of *children / young people* 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 should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **a planned e-safety curriculum should be provided as part of Computing / Health and Wellbeing / other lessons and should be regularly revisited. It may be delivered as an interdisciplinary learning unit;**
- **key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities. The emphasis in such messages should be on children and young people learning to protect themselves and respect others. As appropriate the planned programme should help children / young people understand what Digital Citizenship means and how it relates to the roles and responsibilities outlined in the school's positive behaviour policy;**
- **children / young people 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;**
- **children / young people should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;**
- *children / young people should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices;*
- *in lessons where internet use is pre-planned, it is best practice that children / young people 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 children / young people are allowed to freely search the internet, 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 (for example racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some parents may have extensive knowledge and expertise in this area and be able to support the school.

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

- *curriculum activities;*
- *letters, newsletters, web site, VLE;*
- *parents / carers evenings / sessions;*
- *high profile events / campaigns for example Safer Internet Day;*

- *reference to the relevant web sites / publications for example www.swgfl.org.uk* www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- *providing family learning courses in use of new digital technologies, digital literacy and e-safety;*
- *e-safety mmessages targeted towards grandparents and other relatives as well as parents;*
- *the school website will provide e-safety information for the wider community;*
- *supporting community groups, for example, Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk).*

Education & Training – Staff / Volunteers

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. This will be regularly updated and reinforced. An audit of the e-safety personal learning needs of all staff will be carried out regularly.** *It is expected that some staff will identify e-safety as a professional learning need within the performance review and development process (PRD);*
- **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 Agreements;**
- *the E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (for example from SWGfL / EA / other relevant organisations) and by reviewing guidance documents released by relevant organisations;*
- *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.*

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / 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:

A more detailed Technical Security Template can be found in the appendix.

- **school technical systems will be managed in ways that ensure that the school meets recommended technical requirements** (
- **there will be regular reviews and audits of the safety and security of school technical systems;**
- **servers, wireless systems and cabling must be securely located and physical access restricted;**
- **all users will have clearly defined access rights to school technical systems.** *Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group);*

- a**ll users when deemed old enough/mature enough, approximately P3 upwards will be provided with a username and password** by *(insert name or title) who will keep an up to date record of users and their usernames. Users will be required to change their password every (insert period*
- **the "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher / Principal* or other nominated senior leader and kept in a secure place (e.g. school safe);**

o WIPRO **is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**

- **internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- t*he school has provided enhanced / differentiated user-level filtering through the use of the* WIPRO *filtering programme.*
- *school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *an appropriate system is in place* (to be described) *for users to report any actual / potential e-safety incident to the E-Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed;*
- appropriate security measures are in to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software;
- an agreed policy is in place (to be described) for the provision of temporary access of "guests" (for example trainee teachers, supply teachers, visitors) onto the school system;
- *an agreed policy is in place* (to be described) *regarding the extent of personal use that users (staff / children / young people / community users) and their family members are allowed on school devices that may be used out of school;*
- *an agreed policy is in place* (to be described) *that allows staff to / forbids staff from installing programmes on school devices;*
- *an agreed policy is in place* (to be described) *regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- the school has a set of clear expectations and responsibilities for all users;
- the school adheres to the Data Protection Act principles;
- all users are provided with and accept the Acceptable Use Agreement;
- all network systems are secure and access for users is differentiated;
- where possible these devices will be covered by the school's normal filtering systems, while being used on the premises;
- all users will use their username and password and keep this safe;

- mandatory training is undertaken for all staff;
- children / young people receive training and guidance on the use of personal devices;
- regular audits and monitoring of usage will take place to ensure compliance;
- any device loss, theft, change of ownership of the device will be reported as in the BYOD policy;
- any user leaving the school will follow the process outlined within the BYOD policy;

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children / young people instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children / young people need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Young people should also be aware of potential risks of sharing personal / intimate photographs with friends as they may easily then be spread beyond their intended recipient. The school 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 children / young people about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites, or sending inappropriate /intimate digital images which then may be shared further;**
- in accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (such activity for personal use is exempt under the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *children / young people* in the digital / video images;
- *staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school 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 purpose;*
- *care should be taken when taking digital / video images that children / young people are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;*
- *children / young people must not take, use, share, publish or distribute images of others without their permission;*
- *photographs published on the website, or elsewhere that include children / young people will be selected carefully and will comply with good practice guidance on the use of such images;*
- *children/Young People's 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 children / young people are published on the school website*
- *learners' work can only be published with the permission of the children / young people and parents or carers.*

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 specified lawful purposes;
- adequate, relevant and not excessive;
- accurate and where appropriate, up to date;
- kept no longer than is necessary;
- processed in accordance with the individual's rights;

- secure;
- only transferred outside the European Economic Area with adequate protection.

The school must ensure that:

- **it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;**
- **every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;**
- **all personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing" (see Privacy Note section in the appendix);**
- **it has a Data Protection Policy**
- **it is aware of who the Data Controller within the local authority is;**
- a responsible person (from senior leadership team) is identified as having overall responsibility for ensuring that the school complies with authority guidance and /or data Protection Act in their handling of data, and who identifies and responds to risks related to handling of personal data;
- risk assessments are carried out;
- it has clear and understood arrangements for the security, storage and transfer of personal data;
- individuals have rights of access and there are clear procedures in partnership with the local authority for this to be obtained;
- there are clear and understood policies and routines for the deletion and disposal of data;
- there is a policy for reporting, logging, managing and recovering from information risk incidents;
- there are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
- there are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office;

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 personal data using encryption and secure password protected devices;**

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

- the data must be encrypted and password protected;
- the device must be password protected (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 school 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:

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. Users should be aware that email communications are monitored.** *Staff and children / young people*

	Staff & other adults			Children / young people					All
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed	Not advisedd
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 (needs definition)		✓					✓		
Use of other mobile devices for example tablets, gaming devices	✓				✓				
Use of personal email addresses in school, or on school network (needs explanation)									✓
Use of school email for personal emails									✓
Use of messaging apps			✓						✓
Use of social media		✓				✓			
Use of blogs		✓				✓			

- **users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;**
- **any digital communication between staff and children / young people 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 social media must not be used for these communications;*
- *whole class or group email addresses may be used with younger children. Children / young people will be provided with individual school email addresses for educational use when the school agrees it is appropriate to their age and development.* (Schools may choose to use group or class email addresses for younger age groups);
- *children / young people should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;*
- *personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in the *Code of Professionalism and Conduct,* and the *Standards for Registration* (GTCS).

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school *or* local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues;
- clear reporting guidance, including responsibilities, procedures and sanctions;
- risk assessment, including legal risk.

School staff should ensure that:

- no reference should be made in social media to children / young people, parents / carers or school staff;
- they do not engage in online discussion on personal matters relating to members of the school community;
- personal opinions should not be attributed to the school or local authority;
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior leadership and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination http://www.equalityhumanrights.com/advice-and-guidance/education-providers-schools-guidance/				X	
	threatening behaviour, including promotion of physical violence or mental harm Offensive Behaviour at Football and Threatening Communications (Scotland) Act 2012				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 school or brings the school 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 the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that 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 media		X			
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			X		

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).

Illegal Incidents

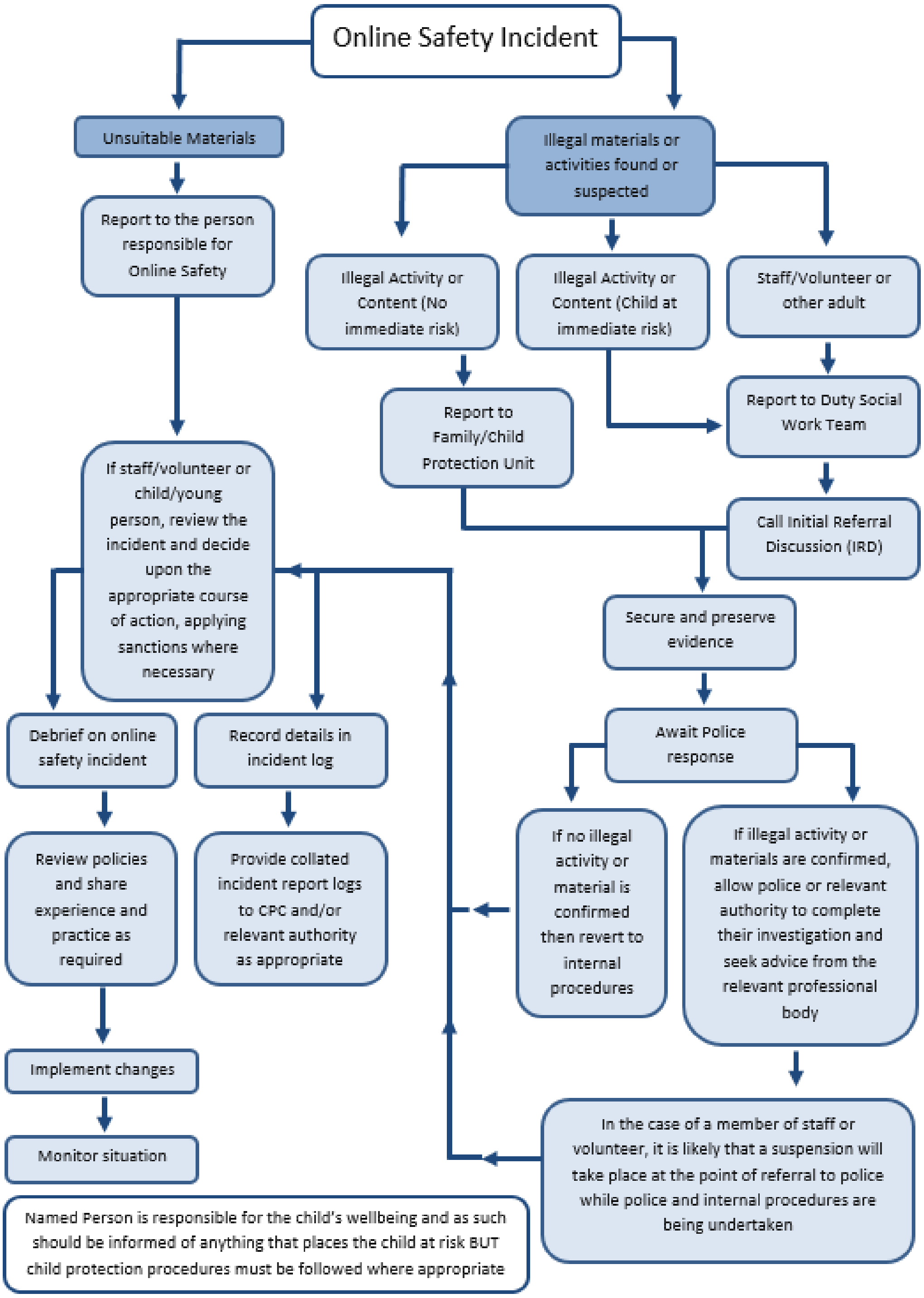
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school 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 concern **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.**


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Family/Child Protection Unit
Report to Duty Social Work Team
Call Initial Referral Discussion (IRD)
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence
Await Police response
Debrief on online safety incident
Record details in incident log
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT child protection procedures must be followed where appropriate

It is important that all of the above steps are taken as they will provide an evidence trail for the school 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.

School Responses to internal incidents

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 as follows:

Children/Young People	**Response**								
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	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 for example detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X		X	X
Unauthorised use of non-educational sites during lessons	X	X	X					X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X					X	
Unauthorised use of social media / messaging apps / personal email	X	X	X					X	
Unauthorised downloading or uploading of files	X	X	X		X			X	
Allowing others to access school network by sharing username and passwords	X	X	X					X	
Attempting to access or accessing the school network, using another student's / pupil's account		X	X			X		X	
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X		X	X
Corrupting or destroying the data of other users		X	X	X		X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X					X	X
Continued infringements of the above, following previous warnings or sanctions			X	X	X		X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X					X	X
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

Staff Response

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X	X						
Unauthorised downloading or uploading of files	X	X						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X					
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules	X	X	X	X	X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with children / young people								
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X						
Using proxy sites or other means to subvert the school's filtering system	X	X	X	X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X		X	X
Breaching copyright or licensing regulations	X							
Continued infringements of the above, following previous warnings or sanctions		X						

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template:

- Members of the SWGfL E-Safety Group.
- Scottish Government
- Christine Knight, Adviser to Scottish Government
- Avon and Somerset Police.
- Representatives of SW Local Authorities.
- Plymouth University Online Safety.
- NEN/ Regional Broadband Grids

Every effort has been made to ensure that the information included in this document is
accurate, as at the date of publication in October 2013. However, SWGfL and Scottish Government
can not guarantee it’s accuracy, nor can they accept liability in respect of the use of the material.

Appendices

Can be found on the following pages:

Digital Citizenship Agreement for Pupils

New technologies have become integral to our lives in today's society, both within schools and in our lives outside school. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Everyone should have an entitlement to safe internet access at all times.

This Agreement is intended to ensure:

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

o **Policy Agreement**

I understand that I must use school ICT systems in a responsible way, to protect myself and respect others and ensure there is no risk 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 that I cannot trust people when I am communicating on-line because they may not be who they say they are. There is ***Stranger Danger*** on line too. I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages.

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

- I understand that the school ICT systems are intended for educational use. I will not use the systems for personal or recreational use unless I have permission to do so.

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

- I will respect others' work and property
- I will be polite and responsible when I communicate with others.

- I will not take or distribute images of anyone without their permission.
- I understand that being a responsible digital citizen means that I have the same standards of relationships and behaviour in an online community as I do in the school community.

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. I understand that, if I do use my own devices in the 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, I will not open any hyperlinks in emails or 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

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.

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

- I understand that the school will respond to incidents of inappropriate behaviour out with school as set out in our school policies.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be held accountable to the school.

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 school ICT systems.

Digital Citizenship Agreement for Pupils Form

This form relates to the *child / young person* 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 school ICT systems.

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

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in the school (when allowed) for example mobile phones, PDAs, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this school for example communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil

Group / Class

Signed

Date

Parent / Carer Countersignature

Signed

Date

Parent / Carer Acceptable Use Agreement 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 technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that children 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 children will have good access to ICT to enhance their learning and will, in return, expect the children to agree to be responsible users. A copy of the Child 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.

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

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above child I give permission for my son / daughter to have access to the internet and to ICT systems at school.

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 the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children and young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Children / young people 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 Data Protection Act 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 can not be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in is exempt under the the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children / young people in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name

Student / Pupil Name

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

Yes / No

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

Yes / No

Signed

Date

Use of Cloud Systems Permission Form

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent' for their children to be able to use these services. It is suggested that schools will incorporate this into their standard acceptable use consent forms sent to parents each year.

The school uses Google Apps for Education for *pupils* and staff. This permission form describes the tools and pupil / student responsibilities for using these services.

The following services are available to each *pupil* and hosted by Google as part of the school's online presence in Google Apps for Education:

Mail - an individual email account for school use managed by the school

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, *pupils* collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils / students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to my child using the school using Google Apps for Education.

Yes / No

Signed

Date

Staff (and Volunteer) Acceptable Use Policy Agreement

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 *children / young people* 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 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 children / young people 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 my use of the ICT systems, email and other digital communications may be monitored.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (for example laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) 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 Highland Council
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I understand the concept of digital citizenship and will model good citizenship online and reinforce messages linking policies and standards on positive behaviour in school and in online communities such as social networks.

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

- I will not inappropriately access, copy, remove or otherwise alter any other user's files.
- 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.
- If I use my personal equipment I will make sure that I do following Highland Council policy
- 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 (for example on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- When I use chat and social networking sites in school it will be in accordance with the school's policies.
- I will only communicate with children / young people and parents / carers using official school systems. Any such communication will be professional in tone and manner. (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 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 mobile 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 not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted.
- 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 which 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 / 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, 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 / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or child / young person 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 school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for 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 the 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 off the premises and my use of personal equipment on the premises 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 Education Authority and/or Governors / Directors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Acceptable Use Agreement for Community Users Template

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- 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 / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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 if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

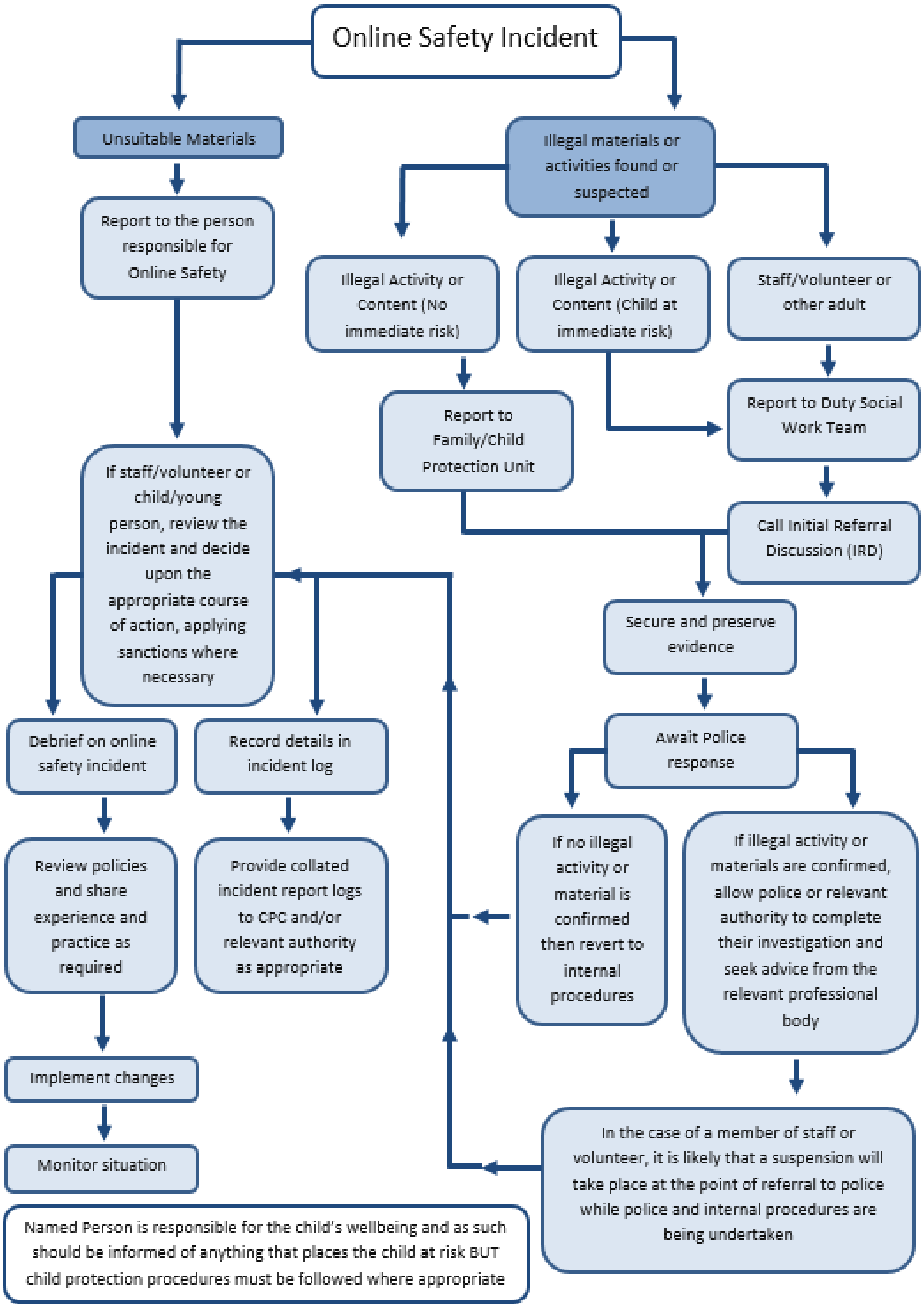
I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name

Signed

Date

Responding to incidents of misuse flowchart


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Family/Child Protection Unit
Report to Duty Social Work Team
Call Initial Referral Discussion (IRD)
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT child protection procedures must be followed where appropriate

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Template Reporting Log

Reporting Log Group						
Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Personal Learning Needs Audit

Training Needs Audit Log
Group .... Date ....

Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

School Technical Security Policy Template (including filtering and passwords) - amended October 2013

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school 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 (other than that 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;
- there is effective guidance and training for users;
- there are regular reviews and audits of the safety and security of school computer systems;
- there is oversight from senior leaders and these have impact on policy and practice.

Highland Council and Kinlochleven High School are confident that the managed service provider WIPRO is fully aware of the Councils E-Safety Policy / Acceptable Use Agreements.

Responsibilities

The overall management of ttechnical security within the school will be the responsibility of Rebecca Machin (Head teacher)

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / 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 will receive guidance and training and will be effective in carrying out their responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Appropriate security measures are in place** to **protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff**
- **All users will have clearly defined access rights to school technical systems.**
- 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. *(See Password section below).*
- The Head teacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software

installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

- *Mobile device security and management procedures are in place*
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *Remote management tools are used by staff to control workstations and view users activity.*
- *An appropriate system is in place for users to report any actual / potential technical incident to the E-Safety Coordinator / Network Manager / Technician*
- An agreed policy will be in place (to be developed) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- *An agreed policy will be in place* (to be developed) *regarding the downloading of executable files and the installation of programmes on school devices by users.*
- *An agreed policy will be in place* (to be developed) *regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.* (see School Personal Data Policy Template in the appendix for further detail)
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.* (see School Personal Data Policy Template in the appendix for further detail).

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- **All school networks and systems will be protected by secure passwords that are regularly changed**
- **The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the *Headteacher and Depute Headteacher* and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts**.
- *Passwords for new users, and replacement passwords for existing users will be allocated by Gordon Milne (Depute Headteacher) Any changes carried out must be notified to the manager of the password security policy (above).*
- All users (adults and young people) 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.
- *Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below.*
- *Requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user* (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

Staff passwords:

- **All staff users will be provided with a username and password** by *Gordon Milne (Depute Headteacher) who will keep an up to date record of users and their usernames;*
- *the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters;*
- *must not include proper names or any other personal information about the user that might be known by others:*
-

  - *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);*
- *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school;*
- should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous passwords *the last four passwords cannot be re-used* created by the same user;
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised;
- should be different for systems used inside and outside of school.

Student / pupil passwords

- **All users will be provided with a username and password** by *Gordon Milne (Depute Headteacher) who will keep an up to date record of users and their usernames;*
- *users will be required to change their password every 60-90 days;*
- children / young people will be taught the importance of password security;
- the complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

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

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

Pupils / students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The responsible person (insert title) will ensure that full records are kept of:

- user Ids and requests for password changes;
- *user log-ons;*
- *security incidents related to this policy.*

Filtering

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, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy is held by WIPRO. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the Head teacher any infringements of the school'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 / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by WIPRO and the Headteacher.*
- *If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.*

Education / Training / Awareness

Children / young people 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:

- *the Acceptable Use Agreement;*
- *induction training;*
- *staff meetings, briefings, Inset.*

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

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 Headteacher who will decide whether to make school level changes (as above).

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to: Rebecca Machin – Headteacher

- *the second responsible person (insert title);*
- *E-Safety Committee;*
- *E-Safety Governor / Governors committee (in independent schools);*
- *external filtering provider / Local Authority / police 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

Further Guidance

Schools may wish to seek further guidance. The following is recommended:

NEN Technical guidance: http://www.nen.gov.uk/advice/266/nen-guidance-notes.html

Somerset Guidance for schools – this checklist is particularly useful where a school / education authority uses external providers for its technical support / security: http://www.360safe.org.uk/Files/Documents/Questions-for-Technical-Support-Somerset.aspx

School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office. In Scotland, the local authority is responsible for data held by schools and institutions. It is important that schools follow the guidance and procedures provided by the authority. 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 protection legislation and relevant regulations and guidance from the Local Authority.

Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained and lawfully processed in accordance with relevant legislation.

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a 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 school community – including *children/ young people* members of staff and parents / carers for example names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data for example class lists, pupil / student progress records, reports, references
- Professional records for example employment history, taxation and 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

The Senior Leadership Team have been allocated responsibility for data related issues within the school 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

Everyone in the school has responsibility for handling protected or sensitive data in a safe and secure manner.

In independent schools, governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The local authority or school (independent sector) is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. Independent schools are responsible for their own registration. http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Information to Parents / Carers

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all children / young people of the data they collect, process and hold on the children / young people, the purposes for which the data is held and the third parties (for example EA, SG, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through the enrolment process and through our annual data check.

Parents / carers of young people who are new to the school will be provided with the privacy notice through the enrolment process

Training & awareness

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

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from the senior leadership team

Risk Assessments

Information risk assessments will be carried out by responsible person in senior leadership team to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts children / young people at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer for example. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The school 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. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User 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 school equipment (this includes computers and portable storage media Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

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
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google docs and Google apps) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. (see appendix for further information and the ICO Guidance: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

As a Data Controller, the local authority is responsible for the security of any data passed to a "third party". In certain circumstance, this is delegated to the school, in relation to information held by the school. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party. Schools should follow the good practice in relation to information-sharing in order to protect and support children as outlined in GIRFEC, and the Quality Indicators "”*How well are we improving the lives of children and young people?”*(Care Inspectorate 2012)

http://www.scotland.gov.uk/Topics/People/Young-People/gettingitright/publications/practice-guide

Evaluating CYP Services with Quality Indicators (Care Inspectorate Scotland) 2012

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site. The *school* recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 individuals have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place (insert details here) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Individuals 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 individual can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school 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 restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location (see earlier section – LA / school policies may forbid such transfer);
- users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (for example family members) when out of school;
- when restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- 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 (if relevant) in this event. (nb. to carry encrypted material is illegal in some countries)

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal 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 (see earlier section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, 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 data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school 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;
- and 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.

Additional issues / documents related to Personal Data Handling in Schools:

Cloud Services

What policies and procedures should be put in place for individual users of cloud-based services?

The school is ultimately responsible for the contract with the provider of the system. Below is a list of questions that should be considered when selecting a cloud services provider;

- How often is the data backed up?
- Does the service provider have a clear process for you to recover data?
- Who owns the data that you store on the platform?
- How does the service provider protect your privacy?
- Who has access to the data?
- Is personal information shared with anyone else? Look out for opt in/opt out features
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that your information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification?
- How will your data be protected? Look out for features that will keep your information safe and secure including Anti-spam, Anti-Virus and Anti-malware…
- How reliable is the system? Look out for availability guarantees.
- What level of support is offered as part of the service? Look out for online and telephone support, service guarantees

SWGfL provides a useful summary of these issues in a document that has been written with the support of Google and Microsoft:

http://www.swgfl.org.uk/News/Content/News-Articles/Cloud-based-products-and-services

Parental permission for use of cloud hosted services

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent'. Normally, schools will incorporate this into their standard acceptable use consent forms sent to parents each year (see suggested wording on "Parent / Carer Acceptable Use Agreement Template")

Privacy and Electronic Communications

Schools should be aware that the Privacy and Electronic Communications Regulations have changed and that they are subject to these changes in the operation of their websites.

Freedom of Information (Scotland) Act 2002 (FoISA)

All local authorities must have a Freedom of Information Policy which sets out how it will deal with FOI requests. Schools must follow the guidance provided by their local authority and refer all requests for FOI to the appropriate officer within the authority. Schools should also have their own policy which should:

- Ensure the provision of advice, guidance, publicity and interpretation of the authority’s policy.
- Consider designating an individual with responsibility for FOI, within the school to provide a single point of reference, and to work in partnership with the responsible officer within the authority. This person should also ensure understand what kind of information can be requested so that they ensure the school will not be compromised by FOI requests.
- Proactively publish the authority’s guidance on FOI with details of how information can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually.
- Ensure that a well managed records management and information system exists in order to comply with requests.
- Ensure a record of refusals and reasons for refusals is kept, allowing schools and the authority to review its access policy on an annual basis.

Model Publication Scheme

The Office of the Scottish Information Commissioner (OSIC) provides authorities with a model publication scheme which they should complete. The school should be aware of the authority’s publication scheme.
Guidance on the model publication scheme can be found at:

http://www.ico.gov.uk/for_organisations/freedom_of_information/guide/publication_scheme.aspx

http://www.scotland.gov.uk/Resource/Doc/1066/0006064.pdf

Further Guidance

ICO guidance can be found at the following link - including a pdf version - updated in September 2012:
http://www.itspublicknowledge.info/ScottishPublicAuthorities/ScottishPublicAuthorities.aspx

School Bring Your Own Devices (BYOD) Template Policy

Under review - to be added

Temporary Access Policy

Under review - to be added

Download Policy

Under review - to be added

Personal Use of School Devices Policy

Under review - to be added

School Policy Template - E-Safety Group Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The e-safety group will seek to include representation from all stakeholders.
The composition of the group should include

- SLT member/s
- Child Protection Coordinator
- Teaching staff member
- Support staff member
- E-safety coordinator
- Parent / Carer
- *Children / young people representation* – for advice and feedback. *Student / pupil voice is essential in the make up of the e-safety committee, but children / young people would only be expected to take part in committee meetings where deemed relevant.*

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

3. CHAIRPERSON

The Group should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying members;
- Inviting other people to attend meetings when required;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

4. DURATION OF MEETINGS

Meetings shall be held every 6 months for a period of 1.5 hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the E-safety Co-coordinator (or other relevant person) with the following [add/delete where relevant]:

- To keep up to date with new developments in the area of e-safety
- To (at least) annually review and develop the e-safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-safety policy
- To monitor the log of reported e-safety incidents (anonymous) to inform future areas of teaching / learning / training
- To coordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through[add/delete as relevant]
- Staff meetings
- Student / pupil forums (for advice and feedback)
- Surveys/questionnaires for children / young people, parents / carers and staff
- Parents evenings

- Website/VLE/Newsletters
- E-safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites)
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyber-bullying for staff and pupils.

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all embers, by agreement of the majority

The above Terms of Reference for Kinlochleven High School have been agreed

Signed by (SLT):

Date:

Date for review:

Acknowledgement

This template terms of reference document is based on one provided to schools by Somerset County Council

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance 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 (Scotland) Act 2000

The Freedom of Information (Scotland) 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 (Scotland) 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.

Regulation of Investigatory Powers Act (Scotland) 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 school 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 Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Sexual Offences (Scotland) Act 2009

The Sexual Offences (Scotland) Act defines consent and allows one party to withdraw it at any stage, whether they initially gave consent or not .The act also gives a legal recognition of male rape.

The Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005

This legislation introduces a new offence of sexual grooming of a person under 16; It also introduces Risk of Sexual Harm Orders (RSHOs) which are designed to protect children from those who display inappropriate behaviour towards them; It introduces a new offence of paying for the sexual services of a person under 18; It introduces new offences of causing, inciting, controlling, arranging or facilitating the provision of sexual services by children or child pornography; It amends current legislation criminalising the taking, possessing and distribution of indecent images of children so that it applies to images of people under 18 rather than only to images of those under 16;

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 school 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 school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Standards in Scotland's Schools Etc Act 2000

Includes framework for school improvement planning and inspection.

Scottish Schools Parental Involvement Act 2006

Guidance on promotion of parental involvement in schools.

Offensive Behaviour at Football and Threatening Communications (Scotland) Act 2012

Focuses on behaviour at Football matches, but also **criminalises the communication of threats of serious violence and threats intended to incite religious hatred, whether sent through the post or posted on the internet.** The Act will only criminalise behaviour likely to lead to public disorder which expresses or incites hatred, is threatening or is otherwise offensive to a reasonable person.

Equalities Act 2010

UK Government legislation applicable to Scotland. Reforms and harmonises equality law and restates previous legislation relating to discrimination and harassment related t o seven personal characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex, and sexual orientation.

Links to other organisations or documents

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

Scottish Government:

ICT in Education.htm

Glow developments

Better relationships, better learning, better behaviour Scottish Government.pdf

UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/

ThinkUKnow

Others:

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

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

Specialist help and support SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

Scottish Government / Scottish Information Commissioners Office:

Biometric recognition technology in schools advice note

Its public knowledge

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

General Teaching Council Scotland:

http://www.gtcs.org.uk/standards/standards.aspx
http://www.gtcs.org.uk/standards/copac.aspx

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

Somerset - Questions for Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

Scottish resources:

http://www.scotland.gov.uk/Topics/Education/Schools/HLivi/childsafety

http://www.scotland.gov.uk/Topics/Education/Schools/Parents

Other:

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
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.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
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
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – 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