SOUTH WEST GRID FOR LEARNING

Cardiff Council

Central South Consortium
Consortiwm Canolbarth y De
Joint Education Service
Gwasanaeth Addysg ar y Cyd

School E-Safety Policies

360 degree safe

the e-safety self review tool

CSC JES School E-Safety Policy

Background / Rationale

Use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

The improper or unsafe use of technology can present challenges to children, young people, volunteers and staff.

Some of the potential risks could include:

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

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a Strategic e-Safety working group made up of Headteachers, High School and Primary School ICT Leaders and Local Authority Staff and has been reviewed by a wide range of relevant stakeholders.

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

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*Insert date_30/09/24_*
The implementation of this e-safety policy will be monitored by the:	*E-Safety Coordinator / Committee,* *Senior Leadership Team* *Other Miss Catrin Evans/SLT_*
Monitoring will take place at regular intervals:	*Annually in the Autumn Term*
The *Governing Body / Governors Sub Committee* 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:	*Once per term*
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:	*Annually in the Autumn Term*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA Schools ICT Strategic Manager,* *LA Safeguarding Officer,* *Police Commissioner's Office*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity (school that manage their own filtering)*
- *Surveys / questionnaires of*
  - *students / pupils (eg CEOP ThinkUknow survey)*
  - parents / carers
  - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regards to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of school.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors / Governors Sub Committee* receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *E-Safety Governor.* The role of the E-Safety Governor will include:

- *regular meetings with the E-Safety Co-ordinator / Officer*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors committee / meeting*

Headteacher and Senior Leaders:

- **The Headteacher is responsible 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 (see below)*.
- *The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant*
- *The Headteacher / 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 Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.*
- **The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents and online safety incident included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinator / Officer:

- leads the e-safety committee
- 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 including how to be alert to the potential misuse of digital media and take responsibility for reporting it appropriately
- liaises with the Local Authority
- liaises with ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (see appendix).
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

Please see Appendix One.

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 school Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /Headteacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction**
- **all digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level *and only carried out using official school systems***
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lesson and other school activities (where allowed) and implement current policies with regard to these devices.
- *in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Designated person for child protection / Child Protection Officer

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

E-Safety Committee

The E-Safety Group provides a consultative group that has wide representation from the *school / academy* community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the *school / academy* this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Body / Directors*.

Members of the *E-safety Group* (or other relevant group) will assist the *E-Safety Coordinator / Officer (or other relevant person, as above)* with:

- the production / review / monitoring of the school e-safety policy / documents.
- *the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.*
- 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 students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Students / pupils:

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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.*

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 / academy (where this is allowed)
- digital media and how to report abuse, misuse or access to inappropriate materials

Visiting Adults and Pupils

Users who access school ICT systems / website / VLE via login as part of the Extended School provision will be expected to sign an AUP before being provided with access to school systems.

Policy Statements

Education – students / pupils

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

E-safety 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 / PHSE / other lessons and should be regularly revisited**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *Students / pupils should be helped to understand the need for the student / pupil 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 students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the 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.*
- *Students should be supported to understand and report unsafe or harmful digital misuse.*

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.

The school will therefore seek to provide information and awareness to parents and carers through: (select / delete as appropriate)

- *Curriculum activities*
- *Letters, newsletters, web site, VLE*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications eg www.swgfl.org.uk* www.saferinternet.org.uk/   http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school / academy will provide opportunities for local community groups / members of the community to gain from the school's / academy'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 messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide e-safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision

Cyberbullying

Cyber bullying has become an increasing concern for schools, parents and children alike. Cyber bullying has traditionally been defined as harassment and victimisation using interactive technology. It is important that we understand the complex nature of cyber bullying to be able to prevent incidents and respond effectively to incidents when they arise. For example, one comment made online becomes bullying when it is repeatedly forwarded or commented on by others, which in turn is seen by multiple people over a sustained period of time. It can often be difficult to gain closure when subject to a cyber bullying incident when the comment or photo can resurface at anytime.

Cyber bullying differs from traditional forms of bullying and can have a significant detrimental impact upon individuals who are targeted by such behaviour. The 24/7 nature of cyber bullying can make it difficult for a target to escape the attacks directed at them. In some cases an individual may not know they are being bullied if they have not seen the content posted about them, but it is important to understand that the intentions of the perpetrator is still to bully the individual in question by posting humiliating and hurtful content.

We promote the positive use of Interactive Technology and Social Media, where pupils are provided with opportunities to discover the benefits social media has to their learning and social development. We understand that it can sometimes be easy to forget that we are talking to real people with real emotions when using social media; as such we encourage and promote responsible use and respectful communications with others online.

All incidents of inappropriate use of social media are taken seriously and we encourage all members of the school community to report any incidents of inappropriate use of social media and interactive technology.

Inappropriate use of social media includes, but not restricted too:

- harassment and intimidation of others,
- sending hateful messages,
- posting inappropriate and unwanted pictures online and;
- creating content which has the potential to hurt, embarrass and humiliate others.
- Sexting
- Online exploitation including sexual abuse

We respond to inappropriate use and bullying online in accordance with the procedures and guidance outlined in our anti-bullying and behaviour policy. Support is provided to all parties involved in incidents of bullying online and parents will be notified following a report of bullying online. Where appropriate we will contact external agencies to obtain further advice, information and provide additional support to individuals if necessary. Restorative approaches will be implemented to resolve any issues of inappropriate use of social media. We understand that in some circumstances there will be a requirement to involve the police. We will liaise with our Police School Liaison Officer for advice on the appropriate route and action to take in these circumstances.

Education & Training – Staff

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

- **A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies**
- *The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at Consortium/ LA / other information / training sessions and by reviewing guidance documents released by BECTA / Consortium / LA and others.*
- *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 as required to individuals as required*

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

Please see Appendix One.

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 / academy'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
- Students / Pupils 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 - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The 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 students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- *Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment,* ***the personal equipment of staff should not be used for such purposes.***
- *Schools are advised to ensure that policies on the storage and destruction of images are in place*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Students / pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Students' / Pupils' full names will not be used in association with photograph, unless enhanced signed consent has been given.*
- *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year* (see Parents / Carers AUP Agreement in the appendix)
- *Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.*

Data Protection

For staff members, please refer to corporate Acceptable Use Policies, Data Protection Policies and school data protection policies.

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:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times / places	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times / places	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons	X							X
Use of mobile phones in social time	X							X
Taking photos on personal mobile phones or other camera devices	X							X
Use of other mobile devices eg tablets, gaming devices	X				X			
Use of personal email addresses in school, or on school network	X							X
Use of school email for personal emails	X						X	
Use of chat rooms / facilities			X					X
Use of instant messaging/messaging apps	X							X
Use of social networking sites		X						X
Use of blogs			X				X	

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

- **The official school email service may be regarded as safe and secure and is monitored.** *Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication concerning school (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems.*
- *The use of personal email addresses, text messaging or public chat / social networking programmes* ***must not be used*** *for professional purposes. Staff should remain professional in tone and content when discussing school online and should not bring the school into disrepute.*
- *Whole class or group email addresses will be used at FP, while students / pupils at KS2 and above can be provided with individual school email addresses for educational use.*

- *Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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				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	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
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 eg Youtube			x			

Responding to incidents of misuse

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

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

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

The flow chart on the next page should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Social Media – Protecting Professional Identity

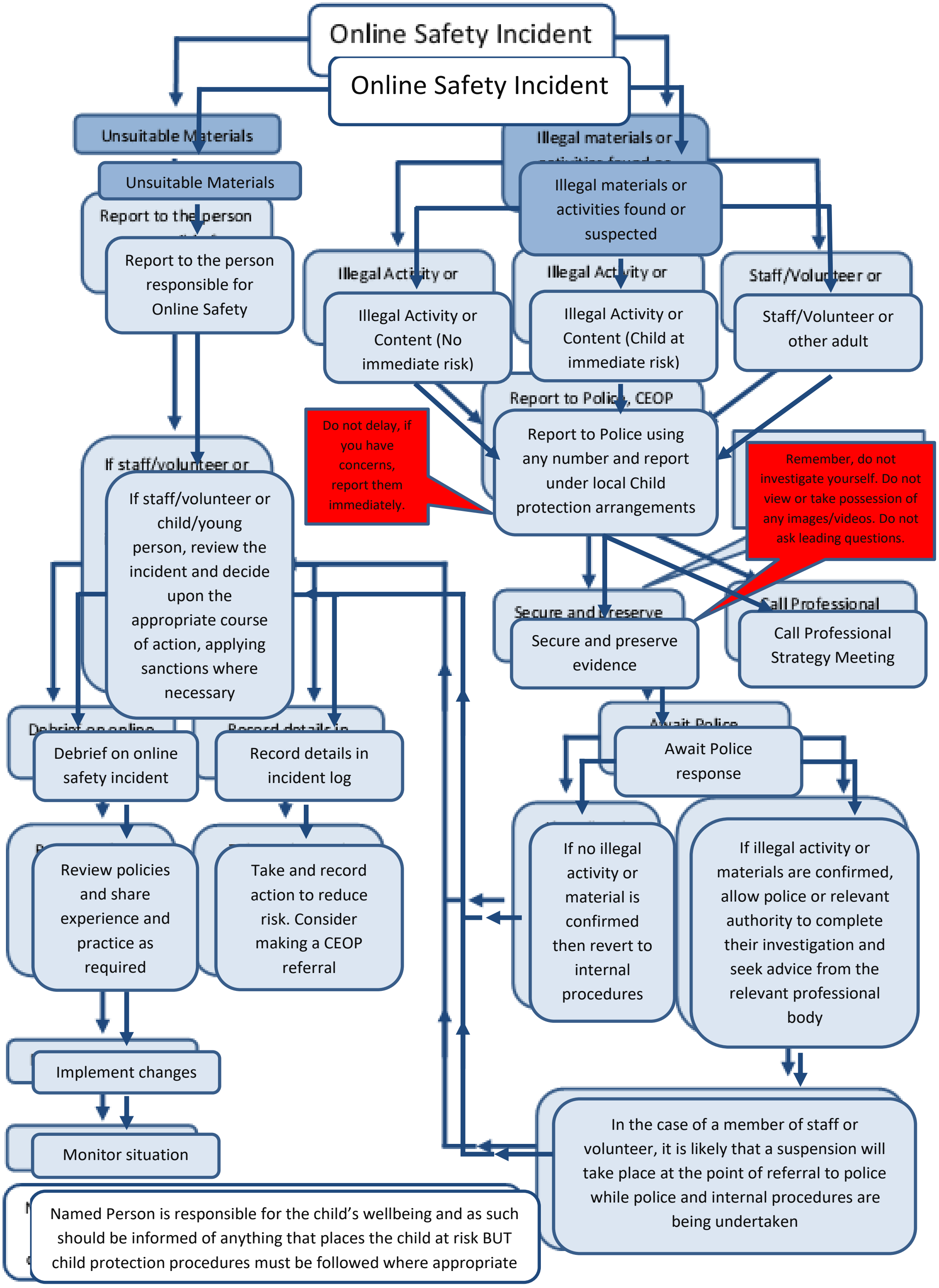
All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, 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 students / pupils, 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 risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review policies and share experience and practice as required
Take and record action to reduce risk. Consider making a CEOP referral
Implement changes
Monitor situation
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
Do not delay, if you have concerns, report them immediately.
Report to Police using any number and report under local Child protection arrangements
Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions.
Secure and preserve evidence
Call Professional Strategy Meeting
Await Police response
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
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

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the "Guidance for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found in the appendix.

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 that follows.

Students / Pupils Actions / Sanctions

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

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	RRefer 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).	✓	✓	✓	✓	✓	□	□	□
Innappropriate personal use of the internet / social networking sites / instant messaging / personal email	□	□	□	□	□	□	□	□
Unauthorised downloading or uploading of files	□	□	□	□	□	□	□	□
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	□	□	□	□	□	□	□	□
Careless use of personal data eg holding or transferring data in an insecure manner	□	□	□	□	□	□	□	□
Deliberate actions to breach data protection or network security rules	□	□	□	□	□	□	□	□
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	□	□	□	□	□	□	□	□
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	□	□	□	□	□	□	□	□
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	□	□	□	□	□	□	□	□
Actions which could compromise the staff member's professional standing	□	□	□	□	□	□	□	□
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	□	□	□	□	□	□	□	□
Using proxy sites or other means to subvert the school's filtering system	□	□	□	□	□	□	□	□
Accidentally accessing offensive or pornographic material and failing to report the incident	□	□	□	□	□	□	□	□
Deliberately accessing or trying to access offensive or pornographic material	□	□	□	□	□	□	□	□
Breaching copyright or licensing regulations	□	□	□	□	□	□	□	□
Continued infringements of the above, following previous warnings or sanctions	□	□	□	□	□	□	□	□

Acknowledgements

Merthyr Tydfil County Borough Council 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:

- SWGFL for their processes, procedures and work to initially create the sample policy that this is based on.
- CSC JES
- All internal and external reviewers and stakeholders
- Consortium Colleagues in Rhondda Cynon Taf, Cardiff, Neath Port Talbot, Bridgend and The Vale of Glamorgan for reviewing and approving this document.
- Merthyr Tydfil Schools ICT Strategic Group e-Safety working group.
- Cardiff Council Schools e-Safety sub-committee
- Merthyr Tydfil Corporate IT Department and Information Security Officer
-
-

Date on which policy was approved by CSC JES Consortium ICT Group: ....

Policy review date: Annually by schools in the Autumn Term. Consortium review to take place in Autumn 2015

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 can not guarantee its accuracy, nor can it accept liability in respect of the use of the material.

Appendix One

Technical
The control, management and monitoring of infrastructure and equipment (internet filtering system and network resources; data; shares; services and software) play a key role in e-safety.

This section of the document outlines schools' and individuals' responsibilities when setting up, connecting and using ICT equipment.

Existing policies and documents outlining conditions of use are in operation, they support and supplement the information and good practice detailed below.

Supporting Documents:

- MTCBC Schools Broadband Terms and Conditions
- MTCBC E-mail Acceptable Use Policy
- MTCBC Internet Acceptable Use Policy
- MTCBC Schools Remote Working Policy
- School's Responsibilities – MTCBC ICT Service Level Agreement

Context

All schools are connected to a shared network, provided for schools. Clients, Servers and Users connecting to the network are administered by the MTCBC ICT Department. Each school has access to a managed wireless and wired network, a filtered internet connection and firewall protection. These services are configured with policies and controls to prevent misuse, malicious attack and to ensure the protection and safety of our data, staff and learners.

The managed service is subject to conditions of use, as outlined in the MTCBC Broadband Terms and Conditions document, and the Schools' Responsibilities section of the ICT Support SLA.

It is the schools' responsibility to ensure that users of ICT systems and equipment are aware of, have access to and have signed the appropriate Acceptable Use Policies.

Where schools have different ICT infrastructures (or elements not maintained by the MTCBC ICT Department) then it is the school's responsibility to ensure:

- Standards of security and controls implemented will need to be equivalent to those outlined in this and other supporting policy documents.
- The security of the schools' Shared Network should not be jeopardised or undermined

In all instances, Schools should name those individuals responsible for upholding the policy(s) implementation and compliance.

Connections to the Schools' Network

- Equipment connected to the Shared Schools Network should be owned by the school and in line with the limitations set out in the Schools ICT Support SLA
- Antivirus: In line with the Schools Broadband Terms and Conditions, it is the school's responsibility to ensure workstations and other devices are protected by up to date virus software.
- Appropriate security measures are in place to protect the servers, networking equipment, work stations, hand held devices, etc from accidental or malicious attempts which might

threaten the security of the school systems and data. These measures should not be circumvented or attempts made to do so.

Internet Filtering

- The school uses and supports the managed filtering service provided by MTCBC ICT Department
- Any filtering issues should be reported immediately to the MTCBC ICT Department (Schools ICT) Helpdesk.
- The School's own Internet Acceptable Use Policy uses the whole of the MTCBC ICT Internet Policy as a baseline – adding policy statements applicable to the local context if needed.
- In accordance with the MTCBC Internet Acceptable Use Policy, school ICT technical or MTCBC ICT staff may monitor and record the activity of users on the school ICT systems. Users are made aware of this in the Acceptable Use Policy.

Access, Controls and Restrictions

- 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.
- All users will have clearly defined access rights to school ICT systems
- Servers, wireless systems and cabling must be securely located and with physical access restricted
- Regular reviews and audits of the safety and security of school ICT systems should be undertaken
- Schools should limit the potential for data loss, Data Security Incidents and the spread of malicious software by controlling the use of removable media.
- Removable media should be encrypted and allocated to individual users.
- Removable media should not be used to transfer data between the Administrative and Curriculum networks
- User may only be granted access to the network/system/software/data resources for which they have a requirement to use.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.

Information Security

- MTCBC/School owned portable ICT equipment should be used in accordance with the Schools Remote Working Policy.
- Personal data about individual staff and learners cannot be sent over the internet (e-mail, attachment or other upload) or taken off the school site unless safely encrypted or otherwise secured.
- The School's own Remote Working Policy Acceptable Use Policy uses the whole of the MTCBC ICT Internet Policy as a baseline – adding policy statements applicable to the local context if needed.
- Information Security Incidents should be logged with the Information Security Officer at the earliest opportunity.
  The School's own E-mail Acceptable Use Policy uses the whole of the MTCBC ICT Internet Policy as a baseline – adding policy statements applicable to the local context if needed.

Appendices

On the following pages you will find a range of supporting policies:

Management:

1. Template acceptable use policy for children and young people (older children)
2. Template acceptable use policy for young children (eg age 8 or younger)
3. Template acceptable use policy for staff and volunteers (including professional identity)
4. Template consent form for parents and carers (including use of images)
5. Template personal data policy
6. Guidelines for Protectively Marking Information

People:

1. Guidance for reviewing internet sites (for suspected harassment and distress)
2. Template reporting log
3. Template training needs audit

Technology

1. Template password security policy
2. Template monitoring log

At the end of this document you will find:

Links to other organisations and documents
Legislation
Glossary
Acknowledgements

Template Policies - Acceptable Use Policy for Older Children (e.g. over the age of 8)

Acceptable Use Policy Agreement

I understand that while I am a member of (insert name) I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the School:

- I will not try to access anything illegal
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within the agreed rules
- I will not deliberately bypass any systems designed to keep the school safer.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school, without permission.
- I will only use social networking, gaming and chat sites with permission (organisations / schools should amend this section to take account of their policy on access to social networking and similar sites)

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name ____________________

Signature ____________________

Date ____________

Template Policies – Acceptable Use Policy for Young Children (e.g. for those aged 8 or younger)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities that an adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……………………………………………

Signed (parent): ……………………………………………..

This AUP is based on one produced by St Mark's Church of England / Methodist Ecumenical VA Primary School, Weston super Mare.

Template Policies –

Acceptable Use Agreement for Staff and Volunteers

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. 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 act responsibly to stay safer while online, being a good role model for younger users.
- effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
- staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

The term "professional" is used to describe the role of any member of staff, volunteer or responsible adult.

For my professional and personal safety I understand that:

- I will ensure that my on-line activity does not compromise my professional responsibilities, nor bring the school into disrepute.
- My use of technology will be monitored.
- When communicating professionally I will use the technology provided by school (eg email and school social media accounts). (you should take account of your policy on communications with children / young people and parents / carers. Staff and volunteers should be aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications).
- These rules also apply when using the school's technology either at home or away from the school site.
- Personal use of school technology is only acceptable with permission.

For the safety of others:

- **I will not access, copy, remove or otherwise alter any other user's files, without authorisation.**
- **I will communicate with others in a professional manner.**
- **I will share other's personal data only with their permission.**
- **I understand that any images I publish will be with the owner's permission and follow the school's code of practice.**
- **I will only use school equipment to record any digital and video images.**

For the safety of the school, I understand that:

- **I will not try to access anything illegal, harmful or inappropriate.**
- **It is my responsibility to immediately report any illegal, harmful or inappropriate incident.**
- **I will not share my online personal information (eg social networking profiles) with the children and young people in my care**
- **I will not deliberately bypass any systems designed to keep school safe.**
- **I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy** (or other relevant policy). **Where personal data leaves the school site, it must be encrypted.**
- **I understand that data protection policy requires that any personal 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 a school policy to disclose such information to an appropriate authority.**
- **Personal passwords and those of other users should always be confidential.**
- **I will not download anything that I do not have the right to use.**
- **I will only use my personal device if I have permission and use it within the agreed rules**
- **I will inform the appropriate person if I find any damage or faults with technology.**
- **I will not attempt to install programmes of any type on the devices belonging to the school, without permission**

Staff / Volunteer Name

Signed

Date

Consent Form for Parents and Carers

A copy of the Children / Young People Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school's expectations of the young people in their care.

Parent / Carers Name:	
Name of Child / Young person:	

As the parent / carer, I give permission for my child to use the school's technology and devices.

I know that my child (over 7 years old) *has signed an Acceptable Use Agreement* and has received guidance to help them understand the importance of online safety.

I understand that the school will take reasonable precautions to ensure that my child will be safer when online, however, I understand that this manages risk but cannot eliminate it.

I understand that my child's online activity will be supervised and monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I understand that the school will take appropriate action in the event of any incidents.

I will encourage my child to adopt safe use of the internet and digital technologies.

Signed		**Date**	

Use of Digital / Video Images

The use of digital / video images plays an important part in our activities. Children / young people, staff and volunteers may use digital cameras or other devices to record evidence of those activities. These images may then be used in Learning Journeys and presentations and may also be used to celebrate success through their publication in newsletters, on the website, social media networks and occasionally in the public media.

The school will comply with the Data Protection Act and request parent / carer permission before taking images of their children. We will also ensure that, wherever possible, full names will not be published alongside images.

It's a great thing to film your child at our events and we know they provide a lot of precious memories. You can support us in keeping our children safe by considering the following:

- *Images and video should be for your own or family's personal use only*
- *Think about privacy and who has the right to see your images, not only of your own child but of others*
- *If you do share the images online, then you must make sure they are limited to immediate family only and not public*
- *If you need help in knowing how to do this then come and have a chat with us*

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

Permission Form

Parent / Carers Name

Name of Child / Young Person

As the parent / carer of the above child, 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 legitimate activities or in publicity that reasonably celebrates success and promotes the work of the school.

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

Signed **Date**

Personal Data Policy

Introduction

Personal Data and Sensitive Personal Data

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

- Personal information about children / young people, members of staff / volunteers and parents and carers eg. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records eg. 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

It is the responsibility of all staff and volunteers 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 or does not need to have access to that data. Anyone who has access to personal data must know, understand and adhere to this the schools data policy and refer to data handling guidelines (supporting policy M6) produced by the information officer.

To clarify, sensitive personal data is defined as:

information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow “good information handling principles”.

Guidance for organisations on the DPA is available on the Information Commissioners Office website: http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Policy Statements

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

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

Responsibilities

The headteacher will keep up to date with current legislation and guidance and will carry out risk assessments

Registration

All schools must register as a Data Controller on the Data Protection Register held by the Information Commissioner. This notification should be reviewed on an annual basis to ensure that the school is still processing data in line with the purposes notified to the ICO.

Training & awareness

Staff and volunteers 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
- Meetings / briefings / training for staff / volunteers
- Day to day support and guidance from the Headteacher.

Risk Assessments

Information risk assessments will be carried out by staff / volunteers to establish key areas of the school where data might be at risk and how the risk could be reduced

Storing personal data

Personal data must be held securely on the school's premises and only accessed by those with permission to do so. Any personal data removed from the premises should have the appropriate level of protection to prevent loss of data. i.e encrypted laptops and memory sticks

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

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place (insert details here) to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required. Such data must be destroyed, rather than deleted and be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, and other (paper based) media must be shredded, incinerated or otherwise disintegrated. Should a 3rd party service be used, then a certificate of destruction should be obtained.

Supporting Policy M6

Guidelines for Protectively Marking Information

Category	PUBLIC CLASSIFICATION	PROTECT CLASSIFICATION	RESTRICTED CLASSIFICATION	CONFIDENTIAL CLASSIFICATION
Examples	• Any policy document that does not give details of security measures; • Professional personal details such as name and job title; • Training documents; • Class list containing name only.	• A single personal record; • Record or information about a single or multiple person(s) which would be subject to the Data Protection Act; • Personally identifiable records such as pupil records, personnel files; staff health records, staff pay records; • General information relating to school operations which if compromised or damaged, may cause inconvenience; • Financial records.	• Minutes of meetings, project reports, bids prior to award, contracts during negotiation; • Health records; • Risk assessments; • Physical security measures used to combat threats.	• Policies or procedures relating to police matters or sensitive health records, including witness or child protection or other individual protective measures; • Network diagrams, procedures or guidelines which discuss details of IT Security standards; • Audit/Monitoring reports;
Impact of Compromise	• No affect to general operations; • No danger, discomfort or embarrassment to the school or individuals; • No breach of statutory	• Minor breach of statutory obligations or duty of confidence; • Cause discomfort or embarrassment to an individual;	• Clear breach of statutory obligations; • Prolonged distress or danger to an individual or risk to personal safety; • Cause danger, discomfort or	• Significant breach of statutory obligations; • Significant harm to the school or local authority; • Significant disruption to operations which could pose

	obligations.	• Reduce an individual’s perception of a school.	embarrassment to many people; • Disruption to school operations or disadvantage a local authority; • Cause financial loss to the school or local authority. •	an increased risk to health and safety. • Cause a financial loss of over £10,000.
Disclosure to other parties	• Freely available without restriction	• Confirm legitimate entitlement exists to share personal data & seek Data Protection & Information Security advice; • Risk assess the exchange methods.		
Email	• Use diligence to protect against accidental compromise; • Take care in addressing email to ensure only intended recipients receive it; • Notify recipients if the email should not be forwarded on to anyone else.	• PROTECT content must be in an attachment and not in the body of the email itself; • Add protective marking to email subject line i.e. before inserting the email subject type, “PROTECT:” so that the recipient is aware of the email classification and how it should be handled; • Ideally password protect the document; • For external mail, use 256bit strength FIPS 140 encryption.	• Encryption MUST be used for sending externally; • Password protected file; • Add protective marking “RESTRICTED” to email subject line; • Content must be in an attachment and not in the body of the email itself.	• Encryption MUST be used for sending externally; • Password protected file. • Add protective marking “CONFIDENTIAL” to email subject line; • Content must be in an attachment and not in the body of the email itself.
Post	• Use due diligence to protect against accidental compromise.	• Should be addressed to a named individual and ideally marked as Private; • Send recorded delivery to track delivery to recipient.	• Clearly mark for the attention of a named recipient; • Send recorded delivery to track delivery to recipient.	• Hand deliver or use trusted courier service that requires signature on pickup and receipt, and tracks delivery; • Double envelope with only internal envelope being

				marked as ‘Private & Confidential’; - Use envelopes designed to protect contents.
Faxing	- Use due diligence to protect against accidental compromise; - Verify identity of recipient fax before sending.	- Only send once intended recipient has confirmed they are able to collect the fax immediately.	- Only send once intended recipient has confirmed they are able to collect the fax immediately.	- Do not use fax.
Printing Photocopies & Scans	- Use due diligence to protect against accidental compromise.	- Only make copies when needed; - Shred spoilt or extra copies or put in confidential waste bins; - Collect promptly from the machines; - Ideally use cross cut shredder.	- Only make copies when needed; - Shred spoilt or extra copies or put in confidential waste bins; - Collect promptly from the machines; - Ideally use cross cut shredder.	- Only print the number of copies actually needed; - Number and log extra copies and register details of those receiving them.
Telephones, Conversations & Presentations	- Use due diligence to protect against accidental compromise.	- Avoid discussing details in a public place; - Do not leave details on voicemail; - Remove paper from flipcharts & wipe white boards clean before leaving.	- Avoid discussing details in a public place; - Do not leave details on voicemail; - Remove paper from flip charts & wipe white boards clean before leaving.	- Do not discuss details in public places or write details on white boards or flip charts.
Use of mobile and removable media, e.g. memory sticks.	- Use due diligence to protect against accidental compromise; - Place in a lockable drawer	- Should only be stored on removable media that is password protected and encrypts data stored; - Head Teacher (or other	- Should only be stored on removable media that is password protected and encrypts data stored; - Head Teacher (or other	- Removable media must not be used.

	when not in use; • Persons are responsible for maintaining security; • Only store minimum data necessary.	appropriate person) should authorise data to be stored on memory stick.	appropriate person) should authorise data to be stored on memory stick.	
Mobile Working	• Use due diligence and protect against accidental compromise; • Lock documents and laptops away when not in use.	• Only use approved school equipment; • Login facilities must be used; • Login and password information must not be written down.	• Only used approved school equipment; • Login facilities must be used; • Login password information must not be written down.	• Paper records must be carried and kept in a folder and must not be left unattended at any time; • Head Teacher (or other appropriate person) should authorise mobile working on files classified as CONFIDENTIAL.
Paperwork	• Apply a clear desk policy; • Put documents away when not in use.	• May be left, face down on a desk for short periods during the day; • File away at the end of the day in a locked drawer.	• Should only be left on a desk when being worked on; • File away at the end of the day in a locked drawer.	• Do not leave unattended at any time; • File away in a locked drawer and preferably a room the can be locked.
Filing/Archiving	• Standard office filing and archiving system; • Store electronic files on the network, not a C drive; • Identify any statutory retention periods.	• Ensure records are kept in lockable cabinets.	• Use lockable cabinets; • Take backups and store backup tapes in a lockable safe.	• Store within a restricted network area; • Store in lockable cabinets in a lockable room; • Take backups and store backup tapes in a lockable safe.
Destruction Methods	• Follow normal recycling policy; • Delete electronic files that are no longer needed using	• Cross cut shredder; • Use confidential waste bins to collect paperwork prior to destruction; • CD ROMs can be cut into quarters;		

	standard system facilities.	• Hard disks must be returned to ICT for approved destruction; • Total destruction of all electronic memory or media and paper to the extent that reconstitution is impossible; • Maintain audit records of destruction.
Markings to be used on documents	• No marking required; • Numbering pages is recommended.	• Indicate the marking level in Headers; • Numbering of pages is essential, and should include number of pages (e.g. Page 1 of 5, 2 of 5….).

Guidance for Reviewing Internet Sites (for suspected harassment and distress)

This guidance is intended for use when schools 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 typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police.

Please follow all steps in this procedure:

- 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 school 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
- **Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.**

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

Record of reviewing internet sites (for suspected harassment / distress)

School	
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

Web site(s) address	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

/Reporting Log School..			
Date	Time		Incident Reported by
Incident			
What action was taken?			
Who took the action?			

Training Needs Audit

Training Needs Audit Log
School .... Date ....

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

Password Security Policy

Introduction

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

- users can only access data to which they have permission.
- access to personal data is securely controlled in line with the school's personal data policy

Responsibilities

- **The management of the password security policy will be the responsibility of the *e-Safety Co-ordinator*. Each user (adults and young people from KS2 onwards) should have their own password and be responsible for its security.**
- *Passwords for new users, and replacement passwords for existing users will be allocated by (insert title).*
- *Users will change their passwords every (insert period).*

Training / Awareness

- It is essential that users should be made aware of the need for keeping passwords secure, not written down or shared with anyone else.
- Adult users will be made aware of the password policy:
  - at induction
  - through the Acceptable Use Agreement
- Children / young people will be made aware of the password policy:
  - when joining the school
  - informally through reminders from staff / volunteers
  - through the Acceptable Use Agreement

Policy Statements

All users from KS2 onwards 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.

The following rules apply to the use of passwords:

- **the "master / administrator" passwords for the school should be held by more than one person (including the senior leader), should not be used for day to day use and must be stored securely.**
- *the master/administrator passwords for the Network, Hwb+ and other VLE's, RM Easymail and any other systems as appropriate will also be kept by the schools ICT team/Schools ICT Strategic Manager.*
- *passwords must be changed every xxxx*
- *the password should be a minimum of X characters long and:*
- *should include a mixture of types of character*
- *should not include proper names*
- *temporary passwords e.g. users with new user accounts or replacement passwords will be forced to change the temporary password when they next log-on*
- *there should be an agreed system for requests for password changes.*
- *where users take laptops with personal data off-site these must be encrypted.*

Monitoring Log

Monitoring Log School …………………………………………………					
Date	Programme / Services Monitored	Monitored by	Issues identified	Reported to	Signed

Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:

South West Grid for Learning: **(**SWGfL Safe) - **http://www.swgfl.org.uk/safe**

360 degree safe: **http://www.360safe.org.uk**

Childnet - **http://www.childnet.com**

CEOP - Think U Know **-** **http://www.thinkuknow.co.uk/**

Netsmartz **http://www.netsmartz.org/index.aspx**
Teach Today **http://www.teachtoday.eu/**
Internet Watch Foundation – report criminal content: **http://www.iwf.org.uk/**
UK Council for Child Internet Safety: **http://www.education.gov.uk/ukccis**
Safer Internet Centre: **http://www.saferinternet.org.uk/**

Management

SWGfL Online Safety Planner. – for groups that work with children and young people – this self review tool allows groups that work with children to assess their policy and provision. **http://www.swgfl.org.uk/ospoffline**

SWGfL School e-safety policy templates: **http://www.swgfl.org.uk/Staying-Safe/Content/News-Articles/Creating-an-e-safety-policy--Where-do-you-start-**

Plymouth Early Years E-Safety Toolkit:
http://www.plymouth.gov.uk/early_years_toolkit.pdf

Byron Review ("Safer Children in a Digital World")
http://webarchive.nationalarchives.gov.uk/tna/+/dcsf.gov.uk/byronreview/
Guidance for safer working practice for adults that work with children and young people - **http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/**

The Learning Trust Example Online Safety Policy (Schools):
http://trustnet.learningtrust.co.uk/Trust/forms/ICT/ICT%20Policies/Internet%20Safety%20Policy.pdf

Belfast Computer Clubhouse Example:
http://www.belfastclubhouse.org/word/Membership-Form.doc

Tech Mission Safe Families AUP: **http://www.safefamilies.org/aup.php**

Policies for voluntary groups eg Woodcraft Folk:
http://www.woodcraft.org.uk/safeguarding

Somerset e-sense progression (e-safety curriculum:-
https://slp.somerset.gov.uk/cypd/elim/somersetict/Site%20Pages/Progressions%20-%20eSense.aspx
Ofsted survey: **http://www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-all-by/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/(language)/eng-GB**

Protecting your personal information online:
http://www.ico.gov.uk/~/media/documents/library/data_protection/practical_application/protecting_your_personal_information_online.ashx

Getnetwise privacy guidance: http://privacy.getnetwise.org/

People

CBBC – stay safe: http://www.bbc.co.uk/cbbc/help/home/
Oldham LSCB Youth Council Charter of Young Peoples Digital Rights:
http://www.esafetyweek.info/
NSPCC: http://www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internet-safety/internet-safety_wdh72864.html
Vodafone Parents Guide: http://parents.vodafone.com/
Google guidance for parents: http://www.teachparentstech.org/

E-Parenting tutorials: http://media-wareness.ca/english/parents/internet/eparenting.cfm
Training - SWGfL EPICT: http://swgfl.org.uk/Staying-Safe/Epict/Epict

Training - SQA Internet Safety qualification:
http://www.sqa.org.uk/sqa/34591.html
Practical Participation – Tim Davies: http://www.practicalparticipation.co.uk/yes/
Protecting Professional Identity documents:
http://public.merlin.swgfl.org.uk/establishments/879/PlymouthChildrensServicesICTAdvice/Pages/ProtectingYourProfessionalIdentity.aspx

SWGfL Facebook guidance –
http://www.swgfl.org.uk/Staying-safe/Files/Documents/facebook-6

Digital Citizenship: http://www.digizen.org.uk/

Kent “Safer Practice with Technology”:
http://kentrustweb.org.uk/CS/community/kent_teachers/archive/2009/07/07/safer-practice-with-technology-for-school-staff.aspx

Connect Safely Parents Guide to Facebook:
http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html

Ofcom – Help your children to manage the media:
http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media/
Mobile broadband guidance: http://www.mobile-broadband.org.uk/guides/complete-resource-of-internet-safety-for-kids/
Orange Parents Guide to the Internet:
http://www.orange.co.uk/communicate/safety/10948.htm
O2 Parents Guide: http://www.o2.co.uk/parents
FOSI – Family Online Internet Safety Contract:
http://www.fosi.org/resources/257-fosi-safety-contract.html

Office for Internet Safety (Ireland) – guide for parents: **http://www.internetsafety.ie/website/ois/oisweb.nsf/page/safety-guideparents-en**
Cybermentors (Beat Bullying): **http://www.cybermentors.org.uk/**
Teachernet Cyberbullying guidance:
http://www.digizen.org/resources/cyberbullying/overview

"Safe to Learn – embedding anti-bullying work in schools"
http://www.anti-bullyingalliance.org.uk/tackling_bullying_behaviour/in_schools/law,_policy_and_guidance/safe_to_learn.aspx

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

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

Technology

Kaspersky – advice on keeping children safe - **http://www.kaspersky.co.uk/keeping_children_safe**
Kaspersky - password advice: **www.kaspersky.co.uk/passwords**
CEOP Report abuse button: **http://www.ceop.police.uk/Safer-By-Design/Report-abuse/**
Information Commissioners Office guidance on use of photos in schools: **http://www.ico.gov.uk/youth/sitecore/content/Home/for_the_public/topic_specific_guides/schools/photos.aspx**

Which Parental control guidance: **http://www.which.co.uk/baby-and-child/child-safety-at-home/guides/parental-control-software/**
How to encrypt files: **http://www.dummies.com/how-to/content/how-to-encrypt-important-files-or-folders-on-your-.html**
Get safe on line – Beginners Guide - **http://www.getsafeonline.org/nqcontent.cfm?a_name=beginners_1**
Childnet Parents and Teachers on downloading / music, film, TV and the internet - **http://www.childnet.com/downloading/**

Microsoft Family safety software: **http://windows.microsoft.com/en-US/windows-vista/Protecting-your-kids-with-Family-Safety**
Norton Online Family: **https://onlinefamily.norton.com/**
Forensic Software **http://www.forensicsoftware.co.uk/education/clients.aspx**

Legislation

Schools should be aware of the legislative framework under which this Online 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 event of an online issue or situation.

Computer Misuse Act 1990:

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The 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 Harrassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the context of work with young people, 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.

The Education and Inspections Act 2006

Empowers school Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Ceased to exist in March 2011, though resources are available from National Archives website)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DfE	Department for Education
ECM	Every Child Matters
ESTYN	The office of Her Majesty's Chief Inspector of Education and Training in Wales
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
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
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
NEN	National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
RBC	Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:
SIC	Safer Internet Centre – a partnership of SWGfL, Childnet and the Internet Watch Foundation which receives European Commission funding to organise Safer Internet Day **(SID)** each February and promote safer internet activities.
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

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 CSCJES cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.