



# Digital Safeguarding Policy

October 2018

<b>Date Completed:</b>	October 2018
<b>Review Date:</b>	October 2019
<b>Co-ordinator Signature:</b>	J Sheard
<b>Governor Approval Date:</b>	
<b>Governor Committee:</b>	
<b>Governor Signature :</b>	





## Development / Monitoring / Review of this Policy

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

- Headteacher and DSL - Mrs P Scott
- E-Safety Coordinator (Computing Coordinator) - Mr J Sheard
- Staff - (Deputy Headteacher and Deputy DSL) Mrs E Wright-Jones; (Emotional Health and Wellbeing Lead and Next Deputy DSL) Mrs J Paskin; (Deputy DSL) Mrs D Mould
- Governors / Board
- Parents and Carers

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

## Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body:	
The implementation of this e-safety policy will be monitored by the:	Mr J Sheard (Assistant Head and Computing Coordinator) Mrs P Scott (Head teacher and DSL)
Monitoring will take place at regular intervals:	Annually
The Governing Body 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:	Annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	October 2019
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	The LADO (01902 550661 - Paul Cooper)

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
  - students / pupils
  - 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 the 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard 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 take place out of school.

## Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities 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 receiving regular information about e-safety incidents and monitoring reports.

### Headteacher and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the e-Safety Co-ordinator.
- **The Headteacher and (at least) 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 - included in a later section - "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body disciplinary procedures*).
- The Headteacher / Senior Leaders are responsible for ensuring that the Computing Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / 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 will receive monitoring reports from the Computing Coordinator addressing the quality of e-safety provision in the school



## Computing Coordinator:

- leads the e-safety working group
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Head Teacher and when necessary other outside agencies (e.g. CEOP)
- liaises with school technical staff (including the reporting of unsuitable site content)
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments ([Examples of suitable log sheets may be found later in this document](#)).
- informs Governors of incidents and risks children may be facing
- attends relevant meetings of Governors

## Technical support:

The Technical Staff are responsible for ensuring:

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- although filtering takes place at local authority level, technical support will contact ICTS if there are any reports of unsuitable site content
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Computing Coordinator, or, when appropriate, Headteacher
- that monitoring software / systems are implemented and updated as agreed in school policies

## Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the Headteacher and/or Computing Coordinator for investigation / action / sanction**
- **all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems**
- e-safety issues are embedded in all aspects of the curriculum and other activities (informal conversations are to be had during lessons, as issues arise, referencing the SMART displays)
- students / pupils understand and follow the e-safety and acceptable use policies



- 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 (iPads only), cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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 (**if there are any unsuitable materials, they should contact both the computing coordinator and technical support staff**)

## Child Protection / Safeguarding Designated Person / Officer

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding 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 Group

The E-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and monitoring of the e-safety policy including the impact of initiatives. The group will also be responsible for reporting to the Governing Body.

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

- the production / review / monitoring of the school e-safety policy / documents.
- ensuring that the school is adhering and using the Wolverhampton filtering procedures
- mapping and reviewing the e-safety curricular provision - ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- monitoring improvement actions identified through use of the 360° degree safe self-review tool

## Students / pupils:

- **are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so



- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school's* E-Safety Policy covers their actions out of school, if related to their membership of the school

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website 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





## 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 and should be regularly revisited at the start of every half term with regular discussions during lessons
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the 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 - mobile devices are not to be used during school hours
- in lessons where internet use is pre-planned, it is best practice that 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit - any inappropriate content should be reported using an e-ticket via the staff learning platform
- 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 - an e-ticket should be submitted via the staff learning platform

### 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:

- Curriculum activities
- Letters, newsletters, website, class sites, social media



- Parents / Carers evenings / sessions (Parents made aware of <http://www.childnet.com/parents-and-carers> )
- High profile events / campaigns e.g. Safer Internet Day [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)

## Education – The Wider Community

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

- The school website will provide e-safety information for the wider community
- Parents' evenings will be an opportunity to share e-safety awareness and tips to parents/carers
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool - [www.onlinecompass.org.uk](http://www.onlinecompass.org.uk))

## Education & Training – Staff / Volunteers

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

- **A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.** SWGfL BOOST includes unlimited online webinar training for all, or nominated, staff (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development>) It is expected that some staff may 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 Agreements.** SWGfL BOOST includes an array of presentations and resources that can be presented to new staff (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Resources>)
- The Computing Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required. SWGfL BOOST includes an array of presentation resources that the e-Safety coordinator can access to deliver to staff (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Resources>). It includes presenter notes to make it easy to confidently cascade to all staff

## 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 technology / 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 / or other relevant organisation
- Participation in school training / information sessions for staff or parents, including parents groups, or school assemblies





## Technical – infrastructure / equipment, filtering and monitoring

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

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users will be provided with a username and secure password** by the computing coordinator who will keep an up to date record of users and their usernames. **Users are responsible for the security of their username and should not share this with others.** The school will use group logons for year 1 and below, managed by teaching staff.
- **The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place**
- **The LTT is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed: where appropriate reported directly to the school DSL, otherwise submitting e-tickets in circumstances of inappropriate content.*
- *Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.*
- *Temporary access for “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems may be provided by the LTT team where deemed appropriate by the Headteacher.*
- *Staff should consult the Computing Coordinator and the LTT before downloading new software onto school hardware.*
- *Staff may take school hardware home if agreed with the Headteacher, but must not leave these unattended outside of their home.*



## 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.

As a school, we require that:

- School staff adhere to the Digital Safeguarding Policy
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students are not allowed to bring their own devices in to school, but are advised on safe usage when at home
- Staff are not to use their own devices during school hours, unless used in a staff's break time, in the staffroom (e.g. mobile phones)
- Parents are advised when and how to use their own devices if used in school (e.g. mobile phones, or tablets)
- 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 to Mrs Scott, as well as Mr Sheard
- If external services, such as LTT wish to use their own devices, they are provided with the Acceptable Users Policy when signing in

## Use of digital and video images

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, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. 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 e.g. on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by The GDPR). To respect



- everyone's privacy and in some cases protection, these images can only be published / made publicly available on social networking sites if they contain only their own child.
- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
  - *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
  - *Students / pupils must not take, use, share, publish or distribute images of others without 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 anywhere on a website or blog, particularly in association with photographs.*
  - *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website, other social media, or shared with a third party.*
  - *Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.*

## Data Protection

See the school's GDPR policy.

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

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



## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils				
	Not Allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission & kept in office	Not allowed
<b>Communication Technologies</b>									
Mobile phones may be brought to school		x						x	
Use of mobile phones in lessons					x				
Use of mobile phones in social time			x		x				
Taking photos on mobile phones / cameras					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 messaging apps			x		x				
Use of social media			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. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school / academy email service to communicate with others when in school, or on school / academy systems (eg by remote access).**
- **Users must immediately report, to the nominated person - in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**



- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Students / pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Social Media - Protecting Professional Identity

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 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
- 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.





## 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 usage as follows:

### User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<b>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:</b>	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			



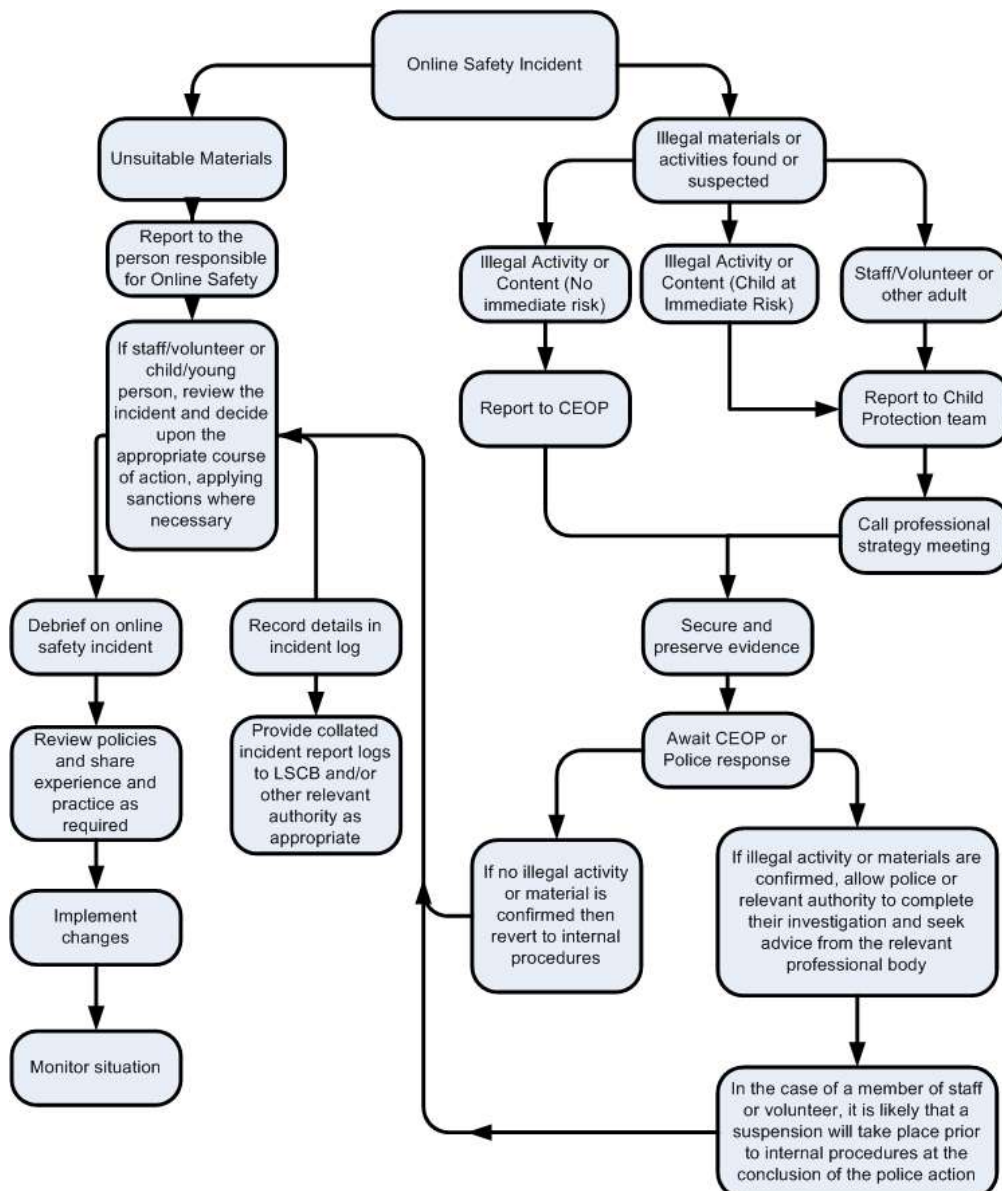
File sharing			X		
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting eg Youtube		X			

## Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

### Illegal Incidents

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



## Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the



- content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse - see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
  - **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
  - **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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



## School Actions & Sanctions

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

### Students / Pupils

### Actions / Sanctions

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





Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X	X	X	X			
---	--	---	---	---	---	---	--	--	--

## Staff

## Actions / Sanctions

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



## Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template and of the 360 degree safe E-Safety Self Review Tool:

- Members of the SWGfL E-Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([esafety@swgfl.org.uk](mailto:esafety@swgfl.org.uk)) and acknowledge its use.

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 it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2013








## Appendices

Copies of the more detailed template policies and agreements, contained in the appendices, can be downloaded from:

<http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy>



## Appendix 1.1 – Foundation AUP

 <h3>E Safety Agreement Foundation</h3>		
These rules help us to stay safe on the Internet		
	We only use the internet when an adult is with us	
	We can click on the buttons or links when we know what they do.	
	We can search the Internet with an adult.	
	We always ask if we get lost on the Internet.	
	We can send and open emails together.	
	We can write polite and friendly emails to people that we know.	

Name ..... Date .....

Signed .....



## Appendix 1.2 – KS1 AUP



# E Safety Agreement KS1

*I want to feel safe all the time.*

*I agree that I will:*

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- only email people I know or if my teacher agrees
- talk to my teacher or a trusted adult before using anything new on the internet or new Apps
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets, or give them my phone number or personal details)
- not load photographs of myself onto the computer
- never agree to meet a stranger

*Anything I do on the computer may be seen by someone else.*

Pupil Name \_\_\_\_\_ Date \_\_\_\_\_

Year Group/Class \_\_\_\_\_





## Appendix 1.3 – KS2 AUP



# E Safety Agreement KS2

\*\*\*\*\*

I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:




- always keep my passwords a secret
- only visit sites which are appropriate to my work at the time
- work in collaboration only with friends and I will deny access to others
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend
- only email people I know or those approved by a responsible adult
- only use email which has been provided by school
- talk to a responsible adult before joining chat rooms or social networking sites
- always keep my personal details private (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult and my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me

I know that once I post a message or an item on the internet then it is completely out of my control.

I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.

Pupil Name \_\_\_\_\_ Date \_\_\_\_\_

Year Group/Class \_\_\_\_\_

\*\*\*\*\*





## Appendix 1.4 – Staff AUP



# E Safety Agreement Staff

Name .....

\*\*\*\*\*  
★ The policy aims to ensure that any communication technology is used  
★ without creating unnecessary risk to users while supporting learning.  
★

★ I agree that I will:

- ★ • Only use personal data securely
- ★ • Implement the schools policy on the use of technology and digital literacy
- ★ • Educate pupils in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- ★ • Educate pupils in the recognition of bias, unreliability and validity of sources
- ★ • Actively educate learners to respect copyright law
- ★ • Only use approved e-mail accounts
- ★ • Only use pupils images or work when approved by parents and in a way that will not enable individual pupils to be identified
- ★ • Only give access to appropriate users when working with blogs or wikis etc...
- ★ • Set strong passwords—a strong password is one which uses a combination of letter, numbers and other permitted signs
- ★ • Report unsuitable content or activities to the e Safety Coordinator
- ★ • Ensure that videoconferencing is supervised appropriately for the learner's age
- ★ • Read and sign the acceptable use policy
- ★ • Pass on any examples of Internet misuse to a senior member of staff
- ★ • Post any supplied E-safety guidance appropriately

★ I agree that I will not:

- ★ • Visit Internet sites, make, post, download, upload or pass on, material remarks, proposals or comments that contain or relate to:
  - ★ ◊ Pornography (including child pornography)
  - ★ ◊ Promoting discrimination of any kind
  - ★ ◊ Promoting racial or religious hatred
  - ★ ◊ Promoting illegal acts
  - ★ ◊ Breach and Local Authority/School policies, e.g. gambling
  - ★ ◊ Do anything which exposes children in my care to danger
  - ★ ◊ Any other information which may be offensive to colleagues
- ★ • Forward chain letters
- ★ • Breach copyright law

★ I accept that my use of the school and Local Authority ICT facilities  
★ may be monitored and the outcomes of the monitoring may be used.  
★

★ Signed ..... Date .....  
★

\*\*\*\*\*



## Appendix 1.5 – Parents' AUP



### E Safety Agreement Parents



Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care. Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name \_\_\_\_\_ Pupil Name \_\_\_\_\_

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

Either: (Years 3 to 6)

I know that my child has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (Foundation and Years 1 and 2)

I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

I will ensure that I only post positive content on any social media relating to the school.

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

Signed \_\_\_\_\_ Date \_\_\_\_\_



## Appendix 1.6 – Visitors' AUP (found on sign in system)



# E Safety Agreement Visitors

\*\*\*\*\*

★ The policy aims to ensure that any communication technology is used  
★ without creating unnecessary risk to users while supporting learning. ★

★ I agree that I will: ★

- ★ • Only use personal data securely
- ★ • Implement the schools policy on the use of technology and digital literacy
- ★ • Only use approved e-mail accounts
- ★ • Only use pupils images or work when approved by parents and in a way that will not enable individual pupils to be identified
- ★ • Only give access to appropriate users when working with blogs or wikis etc...
- ★ • Set strong passwords—a strong password is one which uses a combination of letter, numbers and other permitted signs
- ★ • Report unsuitable content or activities to the Designated Safeguarding Lead (Mrs Scott) or one of the Safeguarding Team
- ★ • Ensure that videoconferencing is supervised appropriately for the learner's age
- ★ • Pass on any examples of internet misuse to a senior member of staff

★ I agree that I will not: ★

- ★ • Visit Internet sites, make, post, download, upload or pass on, material remarks, proposals or comments that contain or relate to:
  - ★ ◦ Pornography (including child pornography)
  - ★ ◦ Promoting discrimination of any kind
  - ★ ◦ Promoting racial or religious hatred
  - ★ ◦ Promoting illegal acts
  - ★ ◦ Breach and Local Authority/School policies, e.g. gambling
  - ★ ◦ Do anything which exposes children in my care to danger
  - ★ ◦ Any other information which may be offensive to colleagues
- ★ • Forward chain letters
- ★ • Breach copyright law

★ By clicking 'Continue', I agree to these conditions. ★

\*\*\*\*\*





## Appendix 2 - Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

### Computer Misuse Act 1990

This Act makes it an offence to:

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

### Data Protection Act 1998

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

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

### Freedom of Information 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 Harassment Act 1997

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

### Protection of Children Act 1978





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

### **Sexual Offences Act 2003**

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

### **Public Order Act 1986**

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

### **Obscene Publications Act 1959 and 1964**

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

### **Human Rights Act 1998**

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

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

### **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.

### **The Education and Inspections Act 2011**

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - <http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

### **The Protection of Freedoms Act 2012**

Requires schools to seek permission from a parent / carer to use Biometric systems



## The School Information Regulations 2012

Requires schools to publish certain information on its website:

<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations>

## Appendix 3 – Glossary of Terms

AUP	Acceptable Use Policy - see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network - works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)



SWGfL

South West Grid for Learning Trust - the Regional Broadband Consortium of SW Local Authorities - is the provider of broadband and other services for schools and other organisations in the SW

TUK

Think U Know - educational e-safety programmes for schools, young people and parents.

VLE

Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP

Wireless Application Protocol