



Perry Wood
PRIMARY & NURSERY SCHOOL

Online Safety Policy

Last Reviewed: September 2025
Review Due: September 2026

Reviewed by: Governors

Contents

Background and rationale.....	3
Policy and leadership	4
Responsibilities: Online Safety lead	4
Responsibilities: governors.....	4
Responsibilities: head teacher	5
Responsibilities: classroom based staff	5
Responsibilities: ICT technician	6
Policy development, monitoring and review	6
Policy Scope	7
Acceptable Use Agreements.....	7
Self Evaluation	8
Whole School approach and links to other policies.....	8
Illegal or inappropriate activities and related sanctions	9
Reporting of Online Safety breaches	12
Use of hand held technology (personal phones and hand held devices).....	13
Use of communication technologies.....	14
Email.....	14
Social networking (including chat, instant messaging, blogging etc)	15
Videoconferencing	15
Use of digital and video images	16
Use of web-based publication tools	17
Website (and other public facing communications).....	17
Learning Platform.....	17
Professional standards for staff communication.....	18
Section B. Infrastructure	18
B.1 Password security	18
Filtering.....	19
Introduction.....	19
Responsibilities.....	19
Education / training / awareness	19
Changes to the filtering system.....	20
Audit / reporting.....	21
Technical security	21
Personal data security (and transfer)	21
Education.....	21
Online Safety education.....	21

Information literacy	22
The contribution of the children to e-learning strategy	22
Staff training	23
Governor training	23
Parent and carer awareness raising	24
Wider school community understanding	24
Appendix 1 – Acceptable Use Agreements	24
Acceptable use policy agreement – pupil	24
Appendix 1b - Acceptable Use Agreement – staff & volunteer	25
Appendix 1c – Parent Permission.....	25
Appendix 2 - Guidance for Reviewing Internet Sites	25
Appendix 3 – Criteria for website filtering.....	27
Appendix 4 - Supporting resources and links.....	28
Cyber Bullying.....	29
Social networking.....	29
Appendix 5 - Glossary of terms.....	31

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming 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 or addictive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Our school's Online Safety policy has been written from a template provided by Worcestershire School Improvement team which has itself been derived from that provided by the South West Grid for Learning.

Policy and leadership

This section begins with an outline of the key people responsible for developing our Online Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT

Responsibilities: Online Safety lead

Our Online Safety coordinator is the person responsible to the head teacher and governors for the day-to-day issues relating to Online Safety. The Online Safety leader: Clare Mahoney

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments as informed by the Head teacher and deputy
- reviews alongside the Head, weekly the output from monitoring software and initiates action where necessary
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

Responsibilities: governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about

Online Safety incidents and monitoring reports. A member of the governing body has taken on the role of Online Safety governor which involves:

- Monitoring of Online Safety incident logs
- Reporting to relevant Governors committee / meeting
- Regular updates with the Online Safety lead (half termly) with an agenda based on:
 - a) monitoring adherence to, and effectiveness of Online Safety and Acceptable Use policies
 - b) monitoring of mechanisms to support pupils, staff and parents facing online safety issues
 - c) regular review of Online Safety training, to ensure it remains relevant and up to date for all stakeholders
 - d) monitoring of mechanisms for educating children to build knowledge, skills and confidence around online safety, and assessing their effectiveness
 - e) monitoring of mechanisms for the education of parents and the whole school community with online safety, and assessing their effectiveness

Responsibilities: head teacher

- The head teacher is responsible for ensuring the safety (including Online Safety) of all members of the school community, though the day to day responsibility for Online Safety is delegated to the Online Safety lead
- The head teacher and another member of the senior management team will be familiar with the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with Online Safety incidents (included in section 2.6 below) and other relevant Local Authority HR / disciplinary procedures)

Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels: this duty is on the individual, not the organisation or the school.
- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school's Acceptable Use Agreement for staff (see Appendix 1)
- they report any suspected misuse or problem to the Online Safety lead
- they undertake any digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) in a fully professional manner and only using official school systems (see A.3.5)
- they embed Online Safety issues in the curriculum and other school activities, also acknowledging the planned Online Safety programme (see section C)

Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school’s ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the Online Safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority Online Safety Policy and guidance)
- users may only access the school’s networks through a properly enforced password protection policy as outlined in the school's e-security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

Policy development, monitoring and review

This Online Safety policy has been developed (from a template provided by Worcestershire School Improvement Service) by a working group made up of:

- School Online Safety Coordinator
- Head teacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors (especially the Online Safety governor)
- Parents and Carers
- Pupils

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Pupil Leadership Team
- INSET Day
- Governors meeting / subcommittee meeting
- Parents evening
- School website / newsletters

Schedule for development / monitoring / review of this policy

The implementation of this Online Safety policy will be monitored by the:	The Online Safety committee under the direction of the Online Safety coordinator
Monitoring will take place at regular intervals:	Once a term.
The governing body will receive regular reports on the implementation of the Online Safety policy generated by the	Report to be sent to each governor meeting

<p>monitoring group (which will include anonymous details of Online Safety incidents) as part of a standing agenda item with reference to safeguarding:</p>	
<p>The Online Safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:</p>	<p>September 2023</p>
<p>Should serious Online Safety incidents take place, the following external persons / agencies should be informed:</p>	<p>Worcestershire Safeguarding Children Board Online Safety representative or Local Authority Designated Officer or Worcestershire Senior Adviser for Safeguarding Children in Education or West Mercia Police</p>

Policy Scope

This policy applies to all members of the school community (including teaching staff, wider workforce, 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 head teachers, to such extent as is reasonable, to regulate the behaviour of 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 Online Safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to accept before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers
- Community users of the school’s ICT system

Acceptable Use Agreements are introduced at parents’ induction meetings and signed by all children as they enter school (with parents possibly signing on behalf of children below Year 2) Children have to accept the agreement every 30 days via a log in requirement.

All employees of the school and volunteers sign when they take up their role in school and have to accept the agreement every 30 days via a log in requirement.

Parents sign once when their child enters the school. The parents’ policy also includes permission for use of their child’s image (still or moving) by the school, permission for their child to use the school’s ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school’s ICT system.

Induction policies for all members of the school community include this guidance.

Acceptable use agreements are on all computers and need to be accepted when logging onto a computer every 30 days for staff and children. Governors, supply staff and volunteers will be required to accept every time they log on.

Self Evaluation

Evaluation of Online Safety is an ongoing process and links to other self evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers ...) are taken into account as a part of this process.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT policies

ICT Policy	How ICT is used, managed, resourced and supported in our school.
Online Safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The Online Safety policy constitutes a part of the ICT policy.
School Systems and Data Security Policy	How we categorise, store and transfer sensitive and personal data and protect school systems. This links strongly and overlaps with the Online Safety policy.

ICT Progressions	Four key documents and associated resources directly relating to learning covering the ICT Curriculum
------------------	---

Other policies relating to Online Safety

Anti-bullying	How your school strives to eliminate bullying – link to cyber bullying
PSHE	Online Safety has links to staying safe
Safeguarding	Safeguarding children electronically is an important aspect of Online Safety. The Online Safety policy forms a part of the school’s safeguarding policy
Relationships	Positive strategies for encouraging Online Safety and sanctions for disregarding it.
Use of images	WCC guidance to support the safe and appropriate use of images in schools and settings

Curriculum policies are to hold the following statement:

We recognise the importance of using ICT to support learning within this subject. ICT may be used for research, recording, photographing etc. Before children use ICT they will be reminded of Online Safety risks. Children will always use their log in and password when using laptops or computers. Children will need to accept our acceptable use policy before using the device. If children do not abide by the acceptable use policy, the Class Teacher will take relevant action.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school).

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 (illegal - The Protection of Children Act 1978)
- grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
- pornography
- promotion of any kind of discrimination

- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Chestnut Ltd Broadband and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)
- On-line gambling and non educational gaming
- On-line shopping / commerce
- Use of social networking sites (other than in the school’s learning platform or sites otherwise permitted by the school)

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see Appendix 2.

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 indicated on the following pages:

	Refer to:					Inform:	Action:		
<p>Pupil sanctions</p> <p>Schools should edit this table as appropriate to their institution.</p> <p>The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.</p>	Class teacher	SLT	Refer to head teacher	Refer to Police	Online Safety Lead for action re filtering / security etc	Parents / carers	Remove of network / internet access rights	Warning	Further sanction e.g. detention / exclusion

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓				
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓				✓	✓		
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓	✓		✓	
Unauthorised downloading or uploading of files	✓	✓			✓	✓	✓	✓	
Allowing others to access school network by sharing username and passwords	✓	✓	✓		✓	✓	✓	✓	
Attempting to access the school network, using another 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	✓	✓	✓		✓	✓	✓	✓	

	Refer to:					Action:		
<p>Staff sanctions</p> <p>Schools should edit this table as appropriate to their institution. The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.</p>	Line manager	Head teacher	Trust/Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action

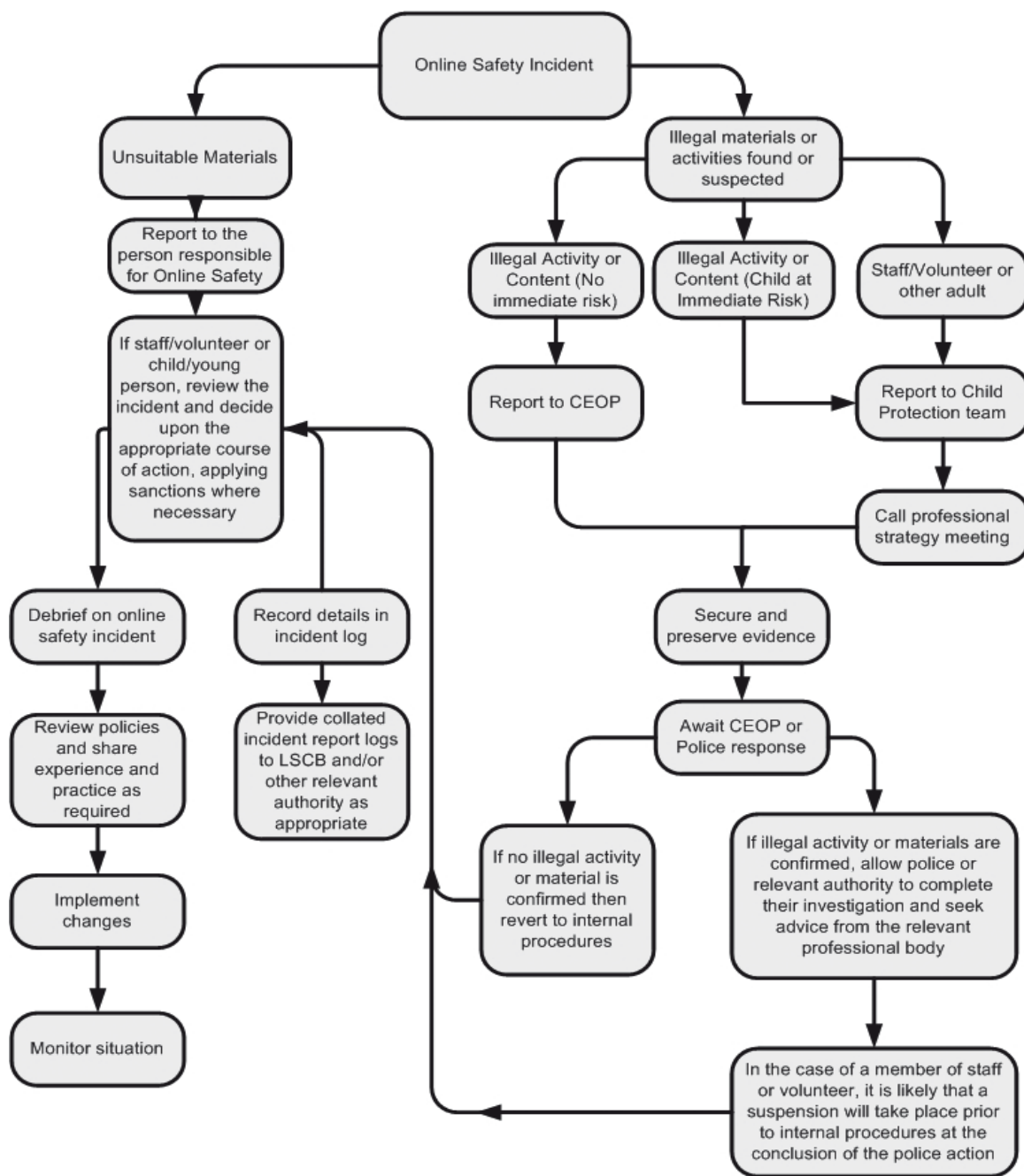
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓		✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓				✓		
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 e.g. 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	✓	✓			✓			✓

Continued infringements of the above, following previous warnings or sanctions

Reporting of Online Safety breaches

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:

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.2.6 of this policy



Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school’s policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
 - a) Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
 - b) Members of staff are free to use these devices outside teaching time.
 - c) A school mobile phone is available for all professional use (for example when engaging in off-site activities) and members of staff should not use their personal device for school purposes except in an emergency.

- Pupils are not currently permitted to bring their personal hand held devices into school.
- Year 5 and 6 children who walk to and from school alone may have a mobile phone. Written consent from parents needs to be received by the office. Phones must be handed in at office, where phones will be kept in named pouches and collected from at end of day.
- A number of such devices are available in school (e.g. PDA, I-pod Touch) and are used by children as considered appropriate by members of staff.

	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Personal hand held technology It is important that schools review this table in the light of principles agreed within their own establishment.								
Mobile phones may be brought to school	✓					✓		✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on personal phones or other camera devices				✓				✓
Use of hand held devices e.g. PDAs, gaming consoles				✓				✓

NB. But see also Section A.3.3 below re use of personal digital equipment.

Use of communication technologies

Email

Access to email is provided for all users in school via the Worcestershire Learning Gateway using their Global IDs. In addition messaging (and email for staff) is available through the school’s learning platform.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- Pupils normally use only a class email account to communicate with people outside school and with the permission / guidance of their class teacher
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy)
- Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (if they are not blocked by filtering)
- Users must immediately report to their class teacher / Online Safety coordinator – in accordance with the school policy (see sections A.2.6 and A.2.7 of this policy) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.

Use of Email	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
It is important that schools review this table in the light of principles agreed within their own establishment.								
Use of personal email accounts in school / on school network				⚡				⚡
Use of school email for personal emails				⚡				⚡

Social networking (including chat, instant messaging, blogging etc)

Use of social networking tools	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
It is important that schools review this table in the light of principles agreed within their own establishment.								
Use of non educational chat rooms etc				⚡				⚡
Use of non educational instant messaging				⚡				⚡
Use of non educational social networking sites			⚡					⚡
Use of non educational blogs				⚡				⚡

Videoconferencing

Desktop video conferencing and messaging systems linked to WCC Broadband via MS Communicator is the preferred communication option in order to secure a quality of service that meets school curriculum standards.

Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer.

External IP addresses should not be made available to other sites.

Only web based conferencing products that are authorised by the school (and are not blocked by internet filtering) are permitted for classroom use.

Videoconferencing is normally supervised directly by a teacher. In the event of this not being the case pupils must ask permission from the class teacher before making or answering a videoconference call.

Permission for children to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in school (see section A.2.3 and Appendix 1). Only where permission is granted may children participate.

Only key administrators have access to videoconferencing administration areas.

Unique log on and password details for the educational videoconferencing services (such as the Janet booking system) are only issued to members of staff.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should normally only be captured using school equipment; the personal equipment of staff should not usually be used for such purposes. However, where staff judge their own equipment is better suited or is more quickly available they may use it, provided that all images taken are uploaded to school equipment and deleted from personal equipment the same day, or within two working days of returning to school if used off site.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- See also the following section (A.3.4) for guidance on publication of photographs

Use of web-based publication tools Website (and other public facing communications)

Our school uses the public facing website (www.perrywood-gst.org) only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- Only pupil's first names will be used on the website, and only then when necessary.
- Detailed calendars will not be published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
 - a) pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
 - b) where possible, photographs will not allow individuals to be recognised
 - c) written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

Learning Platform

Class teachers monitor the use of the learning platform by pupils regularly during all supervised sessions, but with particular regard to messaging and communication. Staff use is monitored by the super-user/administrator.

User accounts and access rights can only be created by the school administrator. Pupils are advised on acceptable conduct and use when using the learning platform. Only members of the current pupil, parent/carers and staff community will have access to the learning platform.

When staff, pupils, etc leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).

Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the learning platform may be suspended for the user.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carers may be informed.

A visitor may be invited onto the learning platform by the administrator following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the broad Professional Standards for Teachers laid down by the TDA (current until the end of August 2012):

http://www.tda.gov.uk/teacher/developing-career/professional-standards-guidance/~media/resources/teacher/professional-standards/standards_a4.pdf

These will be superseded by the Teachers' Standards as described by the DfE effective from September 2012:

<http://media.education.gov.uk/assets/files/pdf/t/teachers%2ostandards.pdf>

Teachers translate these standards appropriately for all matters relating to Online Safety.

Any digital communication between staff and pupils or parents / carers (email, chat, learning platform etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.
- Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Section B. Infrastructure

B.1 Password security

This is dealt with in detail in our school's E-security Policy. Please refer to that document for more information.

The school's Online Safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see section C of this policy)

Filtering Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from Worcestershire County Council, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

It is recognised that the school can take full responsibility for filtering on site but current requirements do not make this something that we intend to pursue at this moment.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the Online Safety coordinator (with ultimate responsibility resting with the head teacher and governors). They manage the school filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Worcestershire school filtering service must

- be logged in change-control logs
- be reported to a second responsible person (the head teacher / Computing coordinator [if they are not also the Online Safety coordinator] / Online Safety governor) within the time frame stated in section A.1.3 of this policy
- be reported to, and authorised by, a second responsible person prior to changes being made (this will normally be the class teacher who originally made the request for the change).
- All users have a responsibility to report immediately to class teachers / Online Safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's Online Safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).
- Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through Online Safety awareness sessions / newsletter etc.

Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the school Online Safety coordinator.
- The Online Safety coordinator checks the website content to ensure that it is appropriate for use in school.

THEN (if the school is not controlling its own filtering)

- If agreement is reached, the Online Safety coordinator makes a request to the Broadband Team
- The Broadband helpdesk will endeavour to unblock the site within 24 hours. This process can still take a number of hours so teaching staff are required to check websites in advance of teaching sessions.
- School Improvement Service Learning Technologies staff may then be notified of websites that have been unblocked to review them in partnership with the Broadband Team. If sites are found to not be appropriate, access will be discussed with the school and then removed. OR (if the school controls its own filtering)

If agreement is reached the Online Safety coordinator unblocks the site and logs the action in the change-control log to be reported as described above

The Online Safety coordinator will need to apply a rigorous policy for approving / rejecting filtering requests. This can be found in Appendix 3 but the core of this should be based on the site's content:

- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.
- B.2.1e Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the. Monitoring takes place as follows:

- Suzanne Beston, Clare Mahoney and Nicky Barley review the Smoothwall console captures weekly
- "False positives" are identified and deleted.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

Audit / reporting

Filter change-control logs and incident logs are made available to:

- the Online Safety governor within the timeframe stated in section A.1.2 of this policy
- the Worcestershire Safeguarding Children Board on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

Technical security

This is dealt with in detail in IBS School's System and Data Security advice. Please see that document for more information.

Personal data security (and transfer)

This is dealt with in detail in IBS School's System and Data Security advice. Please see that document for more information.

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school (see section C of this policy)

Education

Online Safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

- Online Safety education will be provided in the following ways: A planned Online Safety programme is provided as part of ICT, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and outside school
- We use the resources on the Worcestershire Online Safety website as a source of Online Safety education resources <http://www.wes.networcs.net> (e.g. Hector's World at KS1 and Cyber Café and SAFE social networking at KS2)
- Learning opportunities for Online Safety are built into the Knowledge and Understanding sections of the Worcestershire Primary ICT Progressions where appropriate and are used by teachers to inform teaching plans.
- Key Online Safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement (see Appendix 1) and encouraged to adopt safe and responsible use of ICT both within and outside school.
- 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, encouraging children to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
- Checking the likely validity of the URL (web address)
- Cross checking references (Can they find the same information on other sites?)
- Checking the pedigree of the compilers / owners of the website
- See lesson 5 of the Cyber Café Think U Know materials below
- Referring to other (including non-digital) sources
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- We use the resources on CEOP's Think U Know site as a basis for our Online Safety education <http://www.thinkuknow.co.uk/teachers/resources/>

The contribution of the children to e-learning strategy

It is our general school policy to encourage children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

Pupils play a part in monitoring this policy (see section A.1.1)

Staff training

It is essential that all staff – including non-teaching staff - receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff. An audit of the Online Safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify Online Safety as a training need within the performance management process.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and acceptable use policies which are signed as part of their induction
- The Online Safety Lead will be CEOP trained.
- The Online Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, the WSCB and others.
- All teaching staff have been involved in the creation of this Online Safety policy and are therefore aware of its content
- The Online Safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents, is sought from Worcestershire School Improvement Learning Technologies Team when appropriate

If staff had an Online Safety concern they have many sources of support:

- Discuss with Naomi Matanle as Online Safety lead
- Discuss with Clare Mahoney as Safeguarding lead
- Discuss with Mike McCreedy as Online Safety Governor
- Visit the CEOP website <https://ceop.police.uk/safety-centre/>
- Email the Professional Online Safety helpline helpline@saferinternet.org.uk
- For more information visit the <https://www.saferinternet.org.uk/professionals-online-safety-helpline>

If you had a safeguarding concern related to Online Safety this would need to be recorded on a safeguarding form and given to the Clare Mahoney as Safeguarding lead.

Governor training

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

- Attendance at training provided by the Local Authority (Governor Services or School Improvement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The Online Safety governor works closely with the Online Safety coordinator and reports back to the full governing body (see section A.1.3)

Parent and carer awareness raising

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, web site, learning platform
- Half termly Online Safety articles
- Annual Online Safety presentation/ training
- Relevant information on key issues in the news
- Parents evenings
- Reference to the parents materials on the Worcestershire Online Safety website <http://www.wes.networks.net> or others (see Appendix 4)

Wider school community understanding

The school will offer family learning courses in ICT, media literacy and Online Safety so that parents and children can together gain a better understanding of these issues. Messages to the public around Online Safety should also be targeted towards grandparents and other. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Community Users who access school ICT systems / website / learning platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Agreement (see Appendix 1) before being provided with access to school systems.

Appendix 1 – Acceptable Use Agreements Acceptable use policy agreement – pupil

I understand that while I am a member of Perry Wood Primary and Nursery School and I must use technology in a responsible way.

- I understand that my use of technology will be supervised and monitored.
- I will keep my password and personal information safe and will not use anyone else’s (even with their permission)
- I will take care of and appropriately use the computers and other equipment.
- I know that if I break the rules I may not be allowed to use the IT equipment.
- I will always follow the Online Safety rules of the school. 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.

Appendix 1b - Acceptable Use Agreement – staff & volunteer

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed online safety in my work with young people. I agree to be monitored on any device purchased by Perry Wood through Smoothwall.

Appendix 1c – Parent Permission

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

- I understand that my son / daughter will receive, Online Safety education to help them understand the importance of safe and responsible use of ICT – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that 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 that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.
- 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 Online Safety.

Parent’s signature:	
Date:	

Appendix 2 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs 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:

- I 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. This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software. 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:
 - a) Internal response or discipline procedures
 - b) Involvement by Local Authority or national / local organisation (as relevant).
 - c) 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:
 - a) incidents of ‘grooming’ behaviour
 - b) the sending of obscene materials to a child
 - c) 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 group, 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.

Sample documents for recording the review of and action arising from the review of potentially harmful websites can be found in the PDF version of the SWGfL template Online Safety policy (pages 36-38): http://www.swgfl.org.uk/Files/Documents/esp_template_pdf

Appendix 3 – Criteria for website filtering

ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors ("about us", "our objectives", etc.)
- There are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

CONTENT - Is the website's content meaningful in terms of its educational value?

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for the pupils
- The content of the website is current.

DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- have inappropriate adverts?

ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Appendix 4 - Supporting resources and links

The following links may help those who are developing or reviewing a school Online Safety policy.

General

South West Grid for Learning “SWGfL Safe”

<http://www.swgfl.org.uk/Staying-Safe>

Child Exploitation and Online Protection Centre (CEOP)

<http://www.ceop.gov.uk/>

ThinkUKnow

<http://www.thinkuknow.co.uk/>

ChildNet

<http://www.childnet-int.org/>

InSafe

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

Byron Reviews (“Safer Children in a Digital World”)

<http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews>

Becta – various useful resources now archived

<http://webarchive.nationalarchives.gov.uk/20101102103654/http://www.becta.org.uk>

London Grid for Learning

<http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety>

Kent NGfL

<http://www.kented.org.uk/ngfl/ict/safety.htm>

Northern Grid

<http://www.northerngrid.org/index.php/resources/OnlineSafety>

National Education Network NEN Online Safety Audit Tool

http://www.nen.gov.uk/hot_topic/13/nen-Online-Safety-audit-tool.html

WMNet

<http://www.wmnet.org.uk>

WES Worcestershire Online Safety Site

<http://www.wes.networks.net>

EU kids Online

<http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>

Cyber Bullying

Teachernet “Safe to Learn – embedding anti-bullying work in schools” (Archived resources)

<http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/behavior/tacklingbullying/cyberbullying/>

Anti-Bullying Network

<http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org

<http://www.cyberbullying.org/>

East Sussex Council - Cyberbullying - A Guide for Schools:

<https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx>

CyberMentors: young people helping and supporting each other online

<http://www.cybermentors.org.uk/>

Social networking

Digizen – “Young People and Social Networking Services”:

<http://www.digizen.org.uk/socialnetworking/>

Ofcom Report: Engaging with Social Networking sites (Executive Summary)

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

Connect Safely - Smart socialising:

<http://www.blogsafety.com>

Mobile technologies

“How mobile phones help learning in secondary schools”:

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lstri_report.pdf

“Guidelines on misuse of camera and video phones in schools”

http://www.dundee.gov.uk/dundee-city/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

See also Becta (archived) resources above

Parents’ guide to new technologies and social networking

<http://www.iab.ie/>

Links to other resource providers

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

<http://www.swgfl.org.uk/staying-safe>

BBC Webwise

<http://www.bbc.co.uk/webwise/>

Kidsmart

<http://www.kidsmart.org.uk/default.aspx>

Know It All

<http://www.childnet-int.org/kia/>

Cybersmart

<http://www.cybersmartcurriculum.org/home/>

NCH

<http://www.stoptextbully.com/>

Chatdanger

<http://www.chatdanger.com/>

Internet Watch Foundation

<http://www.iwf.org.uk/media/literature.htm>

Digizen – cyber-bullying films

<http://www.digizen.org/cyberbullying/film.aspx>

London Grid for Learning

<http://www.lgfl.net/esafety/Pages/safeguarding.aspx?click-source=nav-toptlevel>

Appendix 5 - Glossary of terms

AUA Acceptable Use Agreement – see templates earlier in this document

Becta British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are archived and still relevant)

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.

DfE Department for Education

FOSI Family Online Safety Institute

ICT Information and Communications Technology

ICT Mark Quality standard for schools provided by NAACE for DfE

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

IWF Internet Watch Foundation

JANET Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia

KS1; KS2 KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)

LA Local Authority

LAN Local Area Network

Learning platform

An online system designed to support teaching and learning in an educational setting

LSCB Local Safeguarding Children Board

MIS Management Information System

NEN National Education Network – works with the Regional Broadband Consortia (eg WMNet) 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

PDA Personal Digital Assistant (handheld device)

PHSE Personal, Health and Social Education

SRF Self Review Framework – a tool maintained by Naace used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark

SWGfL South West Grid for Learning – the Regional Broadband Consortium of SW
Local Authorities and recognised authority on all matters relating to Online Safety (on whose policy
this one is based)

URL Universal Resource Locator – a web address

WMNet The Regional Broadband Consortium of West Midland Local Authorities – provides support
for all schools in the region and connects them all to the National Education Network (Internet)

WSCB Worcestershire Safeguarding Children Board (the local safeguardin