Wellington Primary School and Nursery

E-Safety Policy

Date of review Sept 2019

Date of next review Sept 2020

Contents

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
- Unauthorised access to / loss of / sharing of personal information
- 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 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 we put in place to keep them safe) and so this policy also sets out how we educate children of 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 e-safeguarding policy has been written from a template provided by Herefordshire Council's Learning and Achievement Service which has itself been derived from that provided by the South West Grid for Learning.

Section A - Policy and leadership

This section begins with an outline of the **key people responsible** for developing our E-Safety Policy and keeping everyone safe with Computing. It also outlines the core responsibilities of all users of Computing 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**

A.1.1 Responsibilities

- Review and monitor this e-safety policy.
- Consider any issues relating to school filtering (see section B.2.1 of this policy)
- Discuss any e-safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as the Herefordshire Safeguarding Children Board (HSCB).

A.1.2 Responsibilities: e-safety coordinator

Our e-safety coordinator is the head-teacher and responsible to the governors for the day to day issues relating to e-safety. The e-safety coordinator:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school Computing technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments agree timeframe
- meets regularly with e-safety governor to discuss current issues, review incident logs and filtering change control logs
- attends relevant meetings and committees of Governing Body
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively
- has responsibility for passing on requests for blocking / un blocking to the Computing Co-ordinator.
- maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices (see section A.2.8)

A.1.3 Responsibilities: governors

Our 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 e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor which involves:

- regular meetings with the E-Safety Co-ordinator with an agenda based on:

- monitoring of e-safety incident logs
- monitoring of filtering change control logs
- monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices (see section A.2.8)
- reporting to relevant Governors committee / meeting

A.1.4 Responsibilities: head teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The head teacher and another member of the 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 section 2.6 below and relevant Local Authority HR / disciplinary procedures)

A.1.5 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school's Acceptable Use Policy for staff (see appendix 1)
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems (see A.3.5)
- e-safety issues are embedded in the curriculum and other school activities (see section C)

A.1.6 Responsibilities: Computing technician

The Computing Technician is responsible for ensuring that:

- the school's Computing infrastructure is secure and is not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority E-Safety Policy and guidance.
- users may only access the school's networks through a properly enforced password protection policy as outlined in section B.1 of this policy
- shortcomings in the infrastructure are reported to the Computing coordinator or head teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

This e-safety policy has been developed (from a template provided by Herefordshire Council) by a working group made up of:

- School E-Safety Coordinator
- Head teacher / Senior Leaders
- Teachers
- Support Staff
- Governors (especially the e-safety governor)
- Parents and Carers

- Pupils

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

- Staff meetings
- School Parliament
- INSET Day
- Governors meeting / subcommittee meeting
- Parents evening
- School website / newsletters

Schedule for development / monitoring / review of this policy

This e-safety policy was approved by the governing body on:	February 2019
The implementation of this e-safety policy will be monitored by the:	The e-safety committee under the direction of the e-safety coordinator (Head Teacher)
Monitoring will take place at regular intervals:	Once a year
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:	Twice a year
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2020
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Hereford Safeguarding Children Board e-safety representative Herefordshire Police

A.2.2 Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school Computing 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 e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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.

A.2.3 Acceptable Use Policies

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 sign before being given access to school systems.

Acceptable use policies are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers (including permissions to use pupil images / work and to use Computing systems)

Acceptable use policies are signed by all children as they enter school (with parents possibly signing on behalf of children below KS2) Children resign on entering KS2.

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents.

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy

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 schools Computing resources (including the internet) and permission to publish their work. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each year.

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

A.2.4 Self Evaluation

Evaluation of e-safety is an on-going 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.

A.2.5 Whole School approach and links to other policies

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

Core Computing policies

Computing Policy	How Computing is used, managed, resourced and supported in our school
E-Safety Policy	How we strive to ensure that all individuals in school stay safe while using Computing. The e-safety policy constitutes a part of the Computing policy.
E-Security Policy	How we categorise, store and transfer sensitive and personal data. This links strongly and overlaps with this e-safety policy. (GDPR)
The Herefordshire Computing Progression	Four core age specific documents (and associated resources) directly relating to learning and covering the Computing Curriculum. See www.hereford-edu.org.uk/ict

Other policies relating to e-safety

Anti-bullying	How our school strives to illuminate bullying – link to cyber bullying
PSHE	E-Safety has links to this – staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms a part of the school's safeguarding policy
Behaviour	Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

A.2.6 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 Computing kit provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Herefordshire Council and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not 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 follows:

Pupil sanctions

	Refer to class teacher	Refer to e-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator for action	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. loss of Golden Time
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	?	?	?		?	?	?	?	

Staff sanctions

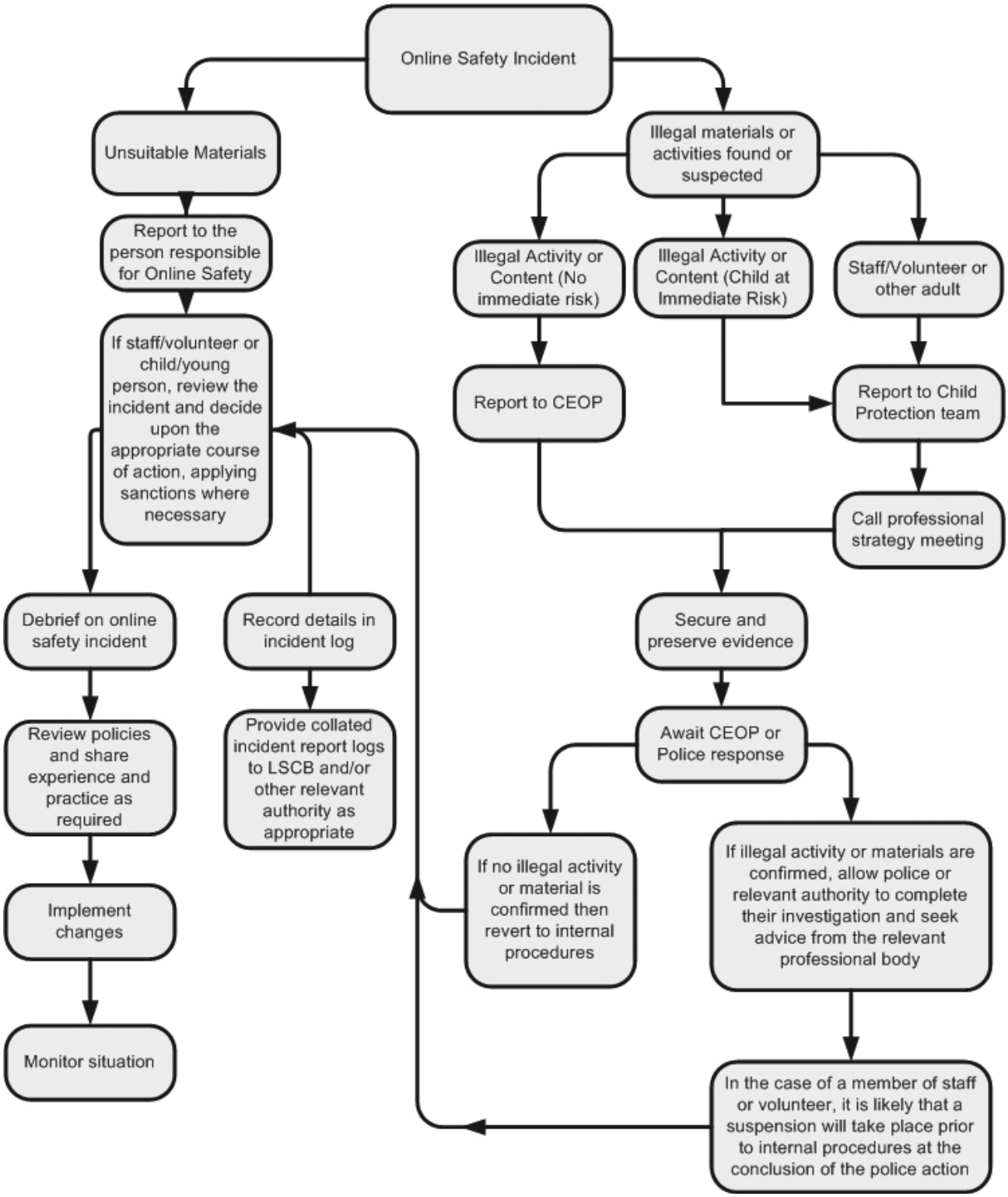
	Refer to line manager	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	?	?	?	?	?	?	?	?
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 eg holding or transferring data in an insecure manner	?	?				?		
Deliberate actions to breach data protection or network security rules	?	?			?	?	?	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	?	?	?			?	?	?

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	?	?	?			?	?	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with 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	?	?	?			?	?	?

A.2.7 Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of Computing resources, 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


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

A.2.8 Electronic Devices - Searching & Deletion (June 2012)

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

Responsibilities

The Headteacher has the authority to carry out searches for and of electronic devices and the deletion of data / files on those devices:

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training / Awareness

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Our search policy

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items.

This E-Safety Policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

The school's policy on the use of mobile devices is set out in section A.3.1 of this policy and the sanctions relating to breaches of these rules in section A.2.6

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or files on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- **Searching with consent** - Authorised staff may search with the pupil's consent for any item.
- **Searching without consent** - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

In carrying out the search:

- The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
- The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.
- There is a limited exception to this rule: authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

- The person conducting the search may not require the pupil to remove any clothing other than outer clothing.

- Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

- A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.
    - 'Possessions' means any goods over which the pupil has or appears to have control – this includes drawers and bags.
- The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.
- Use of force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

Audit / Monitoring / Reporting / Review

The E-Safety coordinator (Head Teacher) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the head teacher and a governor on a termly basis.

A.3.1 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:
    - Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
- Members of staff are responsible for any hand held devices used in school and are aware that these devices must only be used for educational purposes.
- Pupils are not currently permitted to bring their personal hand held devices into school unless permission has been granted.
- A number of such devices are available in school (e.g. ipads) and are used by children as considered appropriate by members of staff.

	Staff / adults				Pupils			
Personal hand held technology	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with permission	Not allowed
Mobile phones may be brought to school	☑							☑
Use of mobile phones in lessons		☑						☑
Use of mobile phones outside lesson time	☑							☑
Taking photos on personal phones or other camera devices				☑				☑
Use of other (non-phone based) hand held devices (e.g. iPods / tablets / gaming consoles)		☑					☑	

A.3.2 Use of communication technologies

A.3.2a - Email

Access to email is provided for all users in school via the intranet page accessible via the web browser (internet Explorer) from their desktop.

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 (eg 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. Pupils have access to an individual email account for communication within school.
- A structured education programme 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 (these may be blocked by filtering).

- Users must immediately report, to their class teacher / e-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 must not respond to any such email.

	Staff / adults				Pupils			
Use of Email	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of personal email accounts in school / on school network		☐						☐
Use of school email for personal emails				☐			☐	

A.3.2b - Social networking (including chat, instant messaging, blogging etc)

	Staff / adults				Pupils			
Use of social networking tools	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
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				☐				☐

A.3.2c - Videoconferencing

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

Equipment connected to the National Education Network (NEN) should use the national E.164 numbering system and display their H323 ID name.

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

Videoconferencing contact information should not be put on the school Website.

Only web based conferencing products that are authorised by the school are permitted for classroom use.

Videoconferencing is normally supervised by a teacher. In the event of this not being the case pupils should ask permission from the supervising 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 schools (see section A.2.3 and Appendix 1) and only where it 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.

Skype is used in school for small group video conferences. The following safeguards are in place:

- The Skype client software is installed only on selected computers
- The use of Skype with children is at all times monitored by staff
- Where the client software is installed, the default "Start Skype when I start Windows" tick is removed (Options – General Settings)
- The Skype shortcut in the Programs menu is removed and a shortcut to launch the software exists only in Common.Staff
- The school uses a single account created in the name of the school
- The client software is closed when not in use.

A.3.3 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 be captured using school equipment, where possible.
- 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

A.3.4 Use of web-based publication tools

A.3.4a - Website (and other public facing communications)

Our school uses Twitter, facebook and the public facing website https://www.wellingtonhereford.com/ 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 should not be posted and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Photographs published that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - 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)

A.3.5 Professional standards for staff communication

In all aspects of their work in our school teachers abide by the **Teachers' Standards** as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf. Teachers translate these standards appropriately for all matters relating to e-safety.

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

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking 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

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

B.2.1 Filtering

B.2.1a - 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.

Our school firewall is managed by D&D

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **e-safety coordinator** (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering, in line with the processes outlined below 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 Herefordshire school filtering service must

- be logged in change control logs
- be reported to a second responsible person within the time frame stated in section A.1.3 of this policy
- be authorised by a second responsible person prior to changes being made
- **All users** have a responsibility to report immediately to class teachers / e-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 be blocked.

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.

B.2.1c - Education / training / awareness

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

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

- signing the AUP (a part of their induction process)
- briefing in staff meetings, training days, memos etc. (from time to time and on-going).

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

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. Monitoring takes place as follows:

- Audit logs of internet activity are generated from time to time in school by the e-safety coordinator or requested of the Herefordshire Computing Schools Helpdesk

B.2.1f - Audit / reporting

Logs of filtering change controls and of filtering incidents are made available to

- the e-safety governor within the timeframe stated in section A.1.3 of this policy
- the e-safety committee (see A.1.1)
- the Herefordshire Safeguarding Children Board (HSCB) on request

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

B.2.2 Personal data security (and transfer)

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) GDPR training has been carried out by all members of staff.

Section C. Education

C.1.1 E-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 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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of Computing, PHSE and other lessons and should be regularly revisited – this will cover both the use of Computing and new technologies in school and outside school
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)

- Learning opportunities for e-safety are built into the Knowledge and Understanding sections of the Herefordshire Primary ICT Progression where appropriate and are used by teachers to inform teaching plans. (www.hereford-edu.org.uk/ict)
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP (see Appendix 1) and encouraged to adopt safe and responsible use of Computing 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

C.1.2 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
- Pupils should 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 e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)

C.1.3 The contribution of the children to e-learning strategy

It is our general school policy to require 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)

C.2 Staff training

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority, the HSCB and others.

- All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.
- External support for training is often sought from Herefordshire's Learning and Achievement Service ICT consultants and from the HSCB

C.3 Governor training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in Computing, e-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 Learning and Achievement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

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

C.4 Parent and carer awareness raising

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 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
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknowco.uk) or others (see Appendix 3)

C.5 Wider school community understanding

The school will offer family learning courses in Computing, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. 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.

Appendix 1 – Acceptable use policy agreement templates

Wellington Primary School's Three Cs of Online Responsibility (EYFS & KS1 AUP)

I agree to keep these computer rules:

Content

- ✓ I always tell an adult if I see something that upsets me on a computer.
- ✓ I ask an adult to help me if I am not sure what to do or if something goes wrong.
- ✓ I only do the things that an adult says are OK.

Contact

- ✓ I only use a computer when there is an adult around.
- ✓ I tell an adult if anyone that I don't know sends me a message or is mean to me.

Conduct

- ✓ I make sure that everything I do on a computer is the best it can be.
- ✓ I am always nice about people and the things they have done at the computer.
- ✓ I take care of the computers.

I understand these computer rules and always do my best to keep them.

My Name:		Date:
R: Signed		
Y1: Signed		
Y2: Signed		

Artwork is from: http://www.saferinternet.org/esafety-kit

Wellington Primary School's Three Cs of Online Responsibility (KS2 AUP)

I agree to be responsible online with:

CONTENT

- ✓ If I find anything online that makes me uncomfortable or that I think we shouldn't have on a school computer I tell an adult so they can sort it out for us
- ✓ I know that it's best if I check with an adult before downloading anything in school

CONTACT

- ✓ I make sure I keep personal information private and help others to do the same
- ✓ I keep all my passwords safe and never use anyone else's (even with their permission)
- ✓ I only use social networking (chat, blogs etc) through the sites the school lets me use
- ✓ If anyone I don't know tries to make contact with me online I ask an adult to give me advice

CONDUCT

- ✓ I show great respect for what others do online and I only post positive comments
- ✓ I make sure that my online image and the way I behave online reflects what a great person I am
- ✓ I make sure that I never share other people's personal information and photographs online unless I check with them first

I am a good, responsible person and proud that I take responsibility for my online behaviour.

I think these are great rules to keep us all safe and I agree to keep them. I promise to do my best to help others to keep these rules too.

Name:		Date:
Y3: Signed		
Y4: Signed		
Y5: Signed		
Y6: Signed		

Artwork is from: http://www.saferinternet.org/esafety-kit

Wellington Primary School Acceptable use policy agreement – staff & volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school Computing systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the Computing systems and other users. I will, where possible, educate the young people in my care in the safe use of Computing and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the Computing systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school Computing systems (laptops, email, VLE, ipads etc) out of school.
- I understand that the school Computing systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the e-safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the e-safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies. (see section A.3.2 of the e-safety policy)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the e-safety policy))
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile Computing devices as agreed in the e-safety policy (see section A.3.1) and then in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school Computing systems except in an emergency (A.3.2).
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies (see e-security policy).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (see e-security policy). Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school Computing equipment in school, but also applies to my use of school Computing systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police (see section A.2.6).

I have read and understand the above and agree to use the school COMPUTING systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

Acceptable use policy agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times. This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using Computing (especially the internet).
- that school Computing 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 Computing to enhance their learning and will, in return, expect them to agree to be responsible users.

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 and assessment.

Child's name	
Parent's name	
Parent's signature:	
Date:	

Permission for my child to use the internet and electronic communication

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

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of Computing – 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 Computing systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

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

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

Parent's signature:	
Date:	

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

In EYFS (Reception children) photos and text evidence will be gathered in a web based assessment format called Orbit Early Years – parents will be invited individually to access their child's information.

Images may also be used to celebrate success through their publication in newsletters, on the school website and in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school community. We will also ensure that, when images are published, young people cannot be identified by name.

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

I agree that if I take digital or video images at school events, where permitted, which include images of children, I will abide by these guidelines in my use of these images. I understand that these will be for my own person use and not shared in any way on the internet (including via social networking sites).

Parent's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website, itunes and in the school's virtual learning environment (VLE)

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

Our school's e-safety Policy, which contains this Acceptable Use Policy Agreement, and the one signed by your child (to which this agreement refers), is available on the school website. Please consult this for more information on any of the above issues.

Acceptable use policy agreement – community user

You have asked to make use of our school's Computing facilities. Before we can give you a log-in to our system we need you to agree to this acceptable use policy.

For my professional and personal safety:

- I understand that the school will monitor my use of the Computing systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school COMPUTING systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's COMPUTING system being withdrawn.

Community user Name:	
Signed:	
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:

- 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 abuse3 then the monitoring should be halted and referred to the Police immediately4. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the 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 arriving from the review of potentially harmful websites can be found in the PDF version of the SWGfL template e-safety policy (pages 36-38):
http://www.swgfl.org.uk/Files/Documents/esp_template_pdf

Appendix 3 – Criteria for website filtering

A. 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 is a contact for further information and questions concerning the site's information and content.

B. 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?

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

- 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
- Is the website current?

D. ACCESSIBILITY - Is the website accessible?

- Loads quickly?
- Does the site require registration or passwords to access it?
- The site does not require usage fees to be paid.

Appendix 4 - Supporting resources and links

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

General

South West Grid for Learning "SWGfL Safe" http://www.swgfl.org.uk/safety/default.asp

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

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

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

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

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

Becta – various useful resources now archived
http://webarchive.nationalarchives.gov.uk/20101102103654/http:/www.becta.org.uk

London Grid for Learning http://cms.lgfl.net/web/lgfl/365

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

Northern Grid http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp

National Education Network NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

WMNet – www.wmnet.org.uk

Cyber Bullying

DCSF - Cyberbullying guidance

http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007

Teachernet http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Teachernet "Safe to Learn – embedding anti-bullying work in schools"

http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/

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

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

East Sussex Council – Cyberbullying - A Guide for Schools:

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

Social networking

Home Office Task Force - Social Networking Guidance -

http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Digizen – "Young People and Social Networking Services": http://www.digizen.org.uk/socialnetworking/

Ofcom Report:

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

Mobile technologies

"How mobile phones help learning in secondary schools":

http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02_a&rid=15482

Mobile phones and cameras:

http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03

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

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

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

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

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

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

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

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

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

Electronic Devices – Searching and deletion (June 2012)

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

It is recommended that Headteachers (and other senior leaders) should be familiar with this guidance.

Relevant legislation:

Education Act 1996

Education and Inspections Act 2006

Education Act 2011 Part 2 (Discipline)

The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012

Health and Safety at Work etc. Act 1974

Obscene Publications Act 1959

Children Act 1989

Human Rights Act 1998

Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Appendix 5 - Glossary of terms

AUP	Acceptable Use Policy – 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 still used)
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
HSCB	Herefordshire Safeguarding Children Board (the local safeguarding board)
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by Becta
ICT Services	Herefordshire ICT Services - provide broadband services and ICT support to Herefordshire schools
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 RBCs.
KS1 ..	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
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 e-safety (on whose policy this one is based)
URL	Universal Resource Locator – posh name for a web address
VLE	Virtual Learning Environment - an online system designed to support teaching and learning in an educational setting,
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)