



**Online Safety Policy for
Hampton Dene Primary School**

Amended	November 2022
Reviewed	
Due for review	November 2024

Online Safety Policy for Hampton Dene Primary School



Contents

Contents	5
Background and rationale	7
Section A - Policy and leadership	8
A.1.1 Responsibilities: the Online Safety committee.....	8
A.1.2 Responsibilities: Online Safety coordinator	8
A.1.3 Responsibilities: governors	9
A.1.4 Responsibilities: head teacher.....	9
A.1.5 Responsibilities: classroom based staff	9
A.1.6 Responsibilities: ICT technician	9
A.2.1 Policy development, monitoring and review	10
Schedule for development / monitoring / review of this policy	11
A.2.2 Policy Scope.....	11
A.2.3 Acceptable Use Policies.....	11
A.2.4 Self Evaluation	12
A.2.5 Whole School approach and links to other policies.....	12
Core ICT policies.....	12
Other policies relating to Online Safety	12
A.2.6 Illegal or inappropriate activities and related sanctions.....	12
A.2.7 Reporting of Online Safety breaches	15
A.2.8 Electronic Devices - Searching & Deletion (June 2012)	16
Responsibilities	17
Training / Awareness	17
Our search policy	17
Electronic devices	18
Deletion of Data.....	18
Audit / Monitoring / Reporting / Review	18
A.3.1 Use of hand held technology (personal phones and hand held devices)	19
A.3.2 Use of communication technologies	21
A.3.2a - Email.....	21
A.3.2b - Social networking (including chat, instant messaging, blogging etc)	22
A.3.2c - Videoconferencing	22
A.3.3 Use of digital images (still and video)	23
A.3.4 Use of web-based publication tools	23

A.3.4a - Website (and other public facing communications)	23
A.3.4b - Virtual Learning Environment (VLE).....	24
A.3.5 Professional standards for staff communication.....	24
A.3.6 Children and Online Safety and away from school.....	26
A.3.7 Reporting procedures for Online Safety away from school.....	26
Section B. Infrastructure	26
B.1 Password security	26
B.2.1 Filtering	26
B.2.2 Technical security	27
B.2.3 Personal data security (and transfer)	27
Section C. Education	28
C.1.1 Online Safety education	28
C.1.2 Information literacy	28
C.1.3 The contribution of the children to e-learning strategy	28
C.2 Staff training	29
C.3 Governor training	29
C.4 Parent and carer awareness raising.....	29
C.5 Wider school community understanding.....	30
Appendix 1 – Acceptable use policy agreement templates	30
Appendix 1a – Acceptable use policy agreement – pupil (KS1)	31
Appendix 1b – Acceptable use policy agreement – pupil (KS2)	32
Appendix 1c - Acceptable use policy agreement – staff & volunteer.....	33
Appendix 1d - Acceptable use policy agreement and permission forms – parent / carer.....	Error! Bookmark not defined.
Appendix 1e - Acceptable use policy agreement – community user	38
Appendix 2 - Guidance for Reviewing Internet Sites	39
Appendix 3 – Criteria for website filtering.....	40
Appendix 4 - Supporting resources and links	41
Sample Templates for incident recording / reporting in school.....	41
Weblinks.....	42
Appendix 5 - Glossary of terms	44

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 Online Safety 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 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**

A.1.1 Responsibilities: the Online Safety committee

Our school has an Online Safety committee led by our Online Safety coordinator and made up of pupils (the class Online Safety officers), teachers and our Online Safety governor. It meets on a termly basis to

- *Review and monitor this Online Safety policy.*
- *Consider any issues relating to school filtering (see section B.2.1 of this policy)*
- *Discuss any Online 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: Online Safety coordinator

Our Online Safety coordinator, Mrs Katherine Adams, is the person responsible to the head teacher and governors for the day to day issues relating to Online Safety. The Online Safety coordinator:

- leads the Online Safety committee
- 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
- meets regularly termly with Online 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 ICT Helpdesk (see section B.2.1)
- 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 Online Safety incidents and monitoring reports. A member of the governing body has taken on the role of Online Safety governor which involves:

- termly meetings with the Online Safety Co-ordinator with an agenda based on:
 - monitoring of Online 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 Online Safety) of members of the school community, though the day to day responsibility for Online Safety is delegated to the Online Safety Co-ordinator
- 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 Online Safety allegation being made against a member of staff. (see flow chart on dealing with Online 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 Online Safety matters and of the current school Online 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 Online 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)
- Online Safety issues are embedded in the curriculum and other school activities (see section C)

A.1.6 Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure is secure and is 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 section B.1 of this policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

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

- *School Online Safety Coordinator*
- *Head teacher / Senior Leaders*
- *Teachers*
- *Governors (especially the Online Safety governor)*

Schedule for development / monitoring / review of this policy

This Online Safety policy was approved by the governing body on:	
The implementation of this Online Safety policy will be monitored by the:	<i>The Online Safety committee under the direction of the Online Safety coordinator</i>
Monitoring will take place at regular intervals:	<i>Once a year</i>
The governing body will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	<i>Once a year</i>
The Online 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 Online Safety or incidents that have taken place. The next anticipated review date will be:	<i>March 2022</i>
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	<i>Hereford Safeguarding Children Board Online Safety representative Herefordshire Police</i>

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 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 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 Online 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 ICT systems)

- Community users of the school's ICT system

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.

For children in EYFS and KS1 parents may sign on behalf of their children

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 ICT 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.

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.

A.2.4 Self Evaluation

Evaluation of Online 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 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 ICT. The Online Safety policy constitutes a part of the ICT policy.
E-Security Policy	How we categorise, store and transfer sensitive and personal data. This links strongly and overlaps with this Online Safety policy.

Other policies relating to Online Safety

Anti-bullying	How our school strives to illuminate bullying – link to cyber bullying
PSHE	Online Safety has links to this – 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
Behaviour	Linking to positive strategies for encouraging Online 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 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 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 Online Safety coordinator	Refer to head teacher	Refer to Police	Refer to Online Safety coordinator	Inform parents / carers	Removal of network / internet access	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	✓	✓	✓		✓	✓	✓	✓	

Staff sanctions

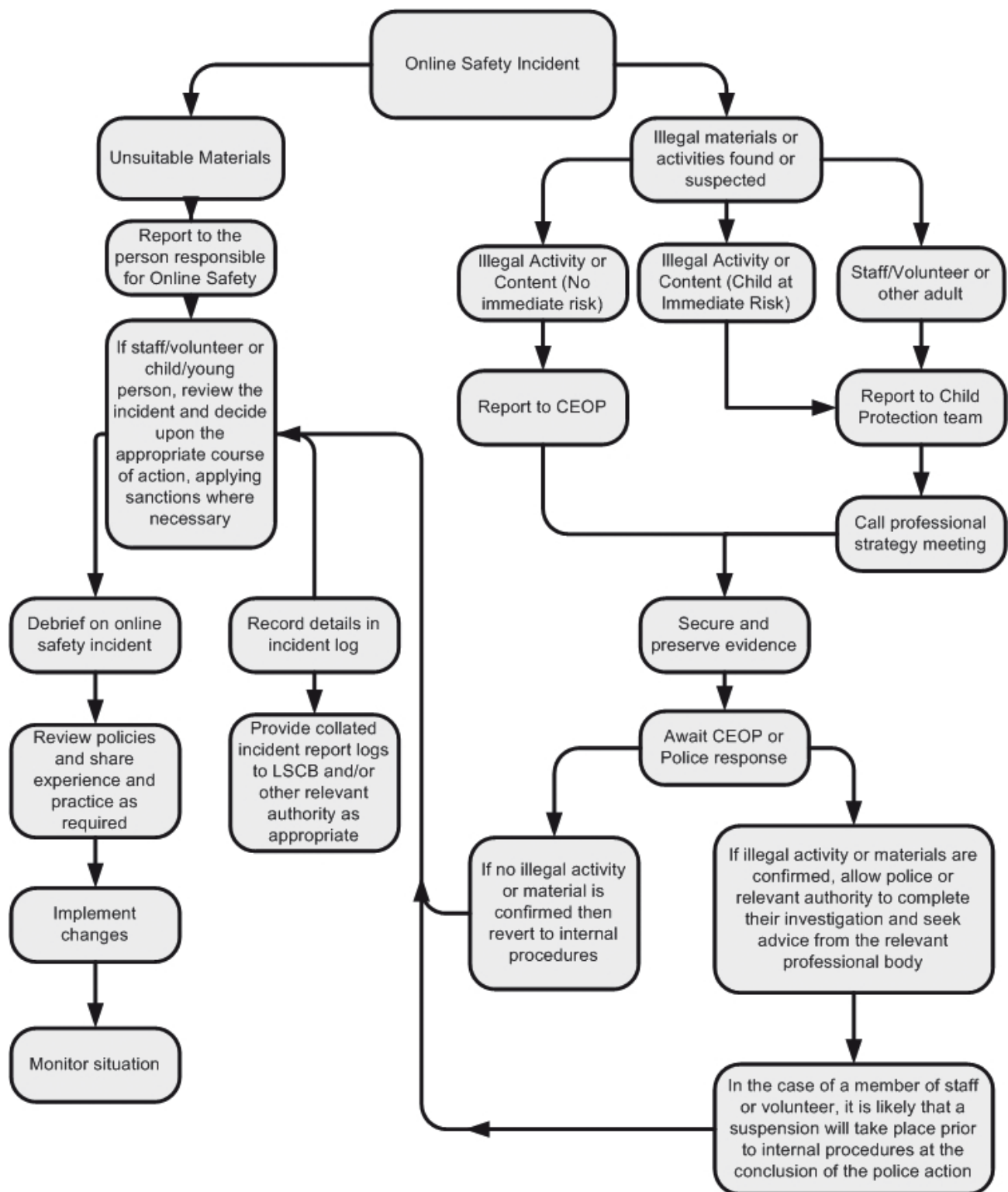
	Refer to line manager	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section 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 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



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 authorised senior members of staff 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 Online 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 desks, lockers 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 Online Safety coordinator 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 free to use these devices in school, outside teaching time.*
 - *Any staff mobile phone brought into school must be protected with a PIN code*
 - *Staff will not normally use their personal phone for taking photographs of children. If they do use their own camera (not a phone) images are captured to a school memory card which is left in school.*
- *Pupils are not currently permitted to bring their personal hand held devices into school except on specific occasions.*
- *Pupils that bring devices into school must hand their device to office staff in the morning so that the device is kept secure within school hours and collect at the end of the school day.*

	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with permission	Not allowed
Personal hand held technology								
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.3.1 Use of Mobile Technology (tablets, phones etc)

A.3.1a – School Owned devices allocated to members of staff

- Personal IDs (for individual downloading of appropriate apps) can be used on school owned devices but teacher iPads must always be signed into the teacher's individual school Apple IDs.
- It is not permissible for children to have access to staff tablets unless very carefully supervised.
- All data is removed from tablets before it is allocated to a different member of staff.
- Individual teachers are responsible for ensuring that any data, apps, photographs etc stored on the iPad are appropriate and professional. This is particularly important when mirroring to interactive whiteboards / screens.
- Cloud storage (other than officially endorsed systems) is not used for sensitive data.
- Specific training on tablet security issues is provided for staff using tablets
- Members of staff must report immediately any loss or compromise of the device or data contained on it.
- Our school uses a mobile device management system (MDM) that manages and tracks staff tablets
- Members of staff are encourage to use devices on home Wi-Fi but are required to be vigilant as to possible security breaches with pubic Wi-Fi

A.3.1b – Personally owned staff devices

- Members of staff are permitted to bring their personal mobile devices into school.
- Personal mobile devices should be used in lesson time only in an emergency or extreme circumstances
- Members of staff are free to use these devices in school, outside teaching time (perhaps in designated areas).
- Any staff mobile technology brought into school must be protected with a PIN code
- Members of staff will not normally use their personal phone or tablet for taking photographs or capturing video of children.
- If they use their own camera (not a phone or tablet) images are downloaded to the school network as soon as possible and deleted from the device before it leaves the school site.
- Mobile phones must be set to silent while in school (this applies to visitors as well as staff employed by the school)
- The school is not responsible for the security of personally owned technology
- Members of staff making use of personal devices in school must be prepared to follow the school's acceptable use policy and be aware that the school may request that they are managed by the school / academy's mobile device management system (MDM).
- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the eight principles of the Data Protection Act (<http://dataprotectionact.org/1.html>)

- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All personal devices used in school must be passcode protected.
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices as part of their Online Safety education.
- Regular audits and monitoring of usage will take place to ensure compliance

A.3.1c – School Owned devices used by pupils

- iPads are available for children to use in school
- Age appropriate apps are purchased via Apple's VPP store and deployed with due regard to licensing and copyright.
- We make use of cloud services in other carefully chosen apps
- Parents give their permission for this via the parents' AUP agreement and permissions form (see appendix 1d)

A.3.1d – Personally owned pupil 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:

- Pupils are not currently permitted to bring their personal hand held devices into school except on specific occasions when advertised.
- Where pupils bring mobile phones and/or other mobile devices to school by prior agreement these are stored in the school office during the school day. They should be clearly labelled with the child's name and passcode protected.
- The school cannot be held responsible for loss of or damage to personally owned technology

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
- 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 / 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 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 images (still and video)

- 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 only be captured using school equipment; the personal equipment of staff should not normally be used for such purposes (where staff members' personal cameras, never phones, are used images are captured to a school memory card which remains in school).
- 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
- It is our school's policy, where possible, to allow parents and pupils to take digital images of children at school events and trips unless otherwise advertised. This they do on the understanding that these images are for their own personal use and are not to be shared online including via social networking.

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 the public facing website 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 on the school website 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, newsletters, displays etc and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs / video 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:
 - 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)
 - See also section A.3.3
- 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.3.4b - Remote Learning Environment (Online Distance Learning)

Class teachers monitor the use of Online Learning environments (e.g. Emile Education, MathswithParents, Sumdog, Seesaw etc) by pupils regularly in all areas, but with particular regard to messaging and communication.

Staff use is monitored by the administrator.

User accounts and access rights can only be created by the school administrator and by LA administrators.

Pupils are advised on acceptable conduct (The Three C's) and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to the accounts on the Remote Learning Environments.

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:

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

A visitor may be invited onto the Remote Learning Environment by the administrator (usually the Computing coordinator) following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

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 Online Safety.

Any digital communication between staff and pupils or parents / carers (email, chat, Remote Learning Environments 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 members are not permitted to have pupils, parents or ex-pupils as friends when personally using social networking sites (e.g. Facebook). They must also not post comments / images that relate to school life.

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.

A.3.6 Children and Online Safety and away from school

In all aspects it is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Safeguarding and Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the Hampton Dene code of conduct.

Hampton Dene will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Teachers will post appropriate and educational learning activities and tasks. Pupils will only be able to see their own work and there will be opportunities for the teacher to respond to the pupils' learning.

There will be no requirement for teachers to replicate the schools' Marking and Feedback policy for remote or distance learning.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided by Hampton Dene Primary School to communicate with pupils

A.3.7 Reporting procedures for Online Safety away from school

Children who are being asked to work online have access to reporting routes so they can raise any concerns whilst online. These are highlighted on the school website.

Children and parents/carers will report any Online Safety incidences back to the school via the admin or their teacher's email address.

Our school website also signposts children to age appropriate practical support from the likes of:

- [Childline](#) - for support
- [UK Safer Internet Centre](#) - to report and remove harmful online content
- [CEOP](#) - for advice on making a report about online abuse

School uses email and the school website to ensure parents and carers are aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school (if anyone) their child is going to be interacting with online.

School highlights support for parents and carers to keep their children safe online via the school website, this includes:

- [Internet matters](#) - for support for parents and carers to keep their children safe online
- [London Grid for Learning](#) - for support for parents and carers to keep their children safe online
- [Net-aware](#) - for support for parents and careers from the NSPCC
- [Parent info](#) - for support for parents and carers to keep their children safe online
- [Thinkuknow](#) - for advice from the National Crime Agency to stay safe online
- [UK Safer Internet Centre](#) - advice for parents and carers

Section B. Infrastructure

B.1 Password security

This is dealt with in detail in our schools **E-security Policy**. Please see that document for more information.

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.

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

B.2.1b - 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 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 reported to a second responsible person (*the head teacher / ICT 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

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 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 Online 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 Online Safety newsletters etc.

B.2.1d – Organisation of and changes to the filtering system

Where a member of staff requires access to a website that is blocked under either policy, the process to unblock is as follows:

- *The teacher makes the request to the school Online Safety coordinator, specifying which filtering policy needs altering.*
- *The Online Safety coordinator checks the website content to ensure that it is appropriate for use in this policy.*
- *If agreement is reached, the Online Safety coordinator logs the request with D&D at support@dandd.org.*
- *D&D will endeavour to unblock the site at the time of the request and within 24 hours. This process can still take a number of hours so teaching staff are still asked to check websites in advance of teaching sessions.*
- *Learning and Achievement Service ICT staff will then be notified of all the websites that have been unblocked and will review them in partnership with the information security team. If sites are felt to be inappropriate, access will be discussed with the school and then removed.*

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 Online Safety coordinator or requested from D&D.*

B.2.1f - Audit / reporting

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

- the Online Safety governor within the timeframe stated in section A.1.3 of this policy
- *the Online 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 Technical security

This is dealt with in detail in our schools **E-security Policy**. Please see that document for more information.

B.2.3 Personal data security (and transfer)

This is dealt with in detail in our schools **E-security Policy**. 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)

Section C. Education

C.1.1 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 should be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- *We use the resources provided by SWGFL's Digital Literacy and Digital Citizenship scheme of work for KS1 and KS2 alongside the 'Safe' resources for KS2.*
- Key Online 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 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, 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
- 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

C.1.3 The contribution of the children to Online 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 Online 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 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 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 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 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 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 Learning and Achievement 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)

C.4 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, Remote Learning Environments
- Parents evenings
- Reference to the parent's materials on the Think U Know website (www.thinkuknow.co.uk) or others (see Appendix 3)

C.5 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 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.

Community Users who access school ICT systems / website / Remote Learning Environments as part of the Extended School provision will be expected to sign a Community User AUP (see Appendix 1) before being provided with access to school systems.

Appendix 1a – Acceptable use policy agreement – pupil (KS1)

This is how we stay safe when we use computers:

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

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

My name:		Date
R - Signed (child):		
Y1 - Signed (child):		
Y2- Signed (child):		

Appendix 1b – Acceptable use policy agreement – pupil (KS2)

I understand that while I am a member of Hampton Dene Primary School I must use technology in a responsible way.

For my own personal safety:

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

For the safety of others:

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

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal ICT kit if I have permission and then I will use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
- I will only use social networking, gaming and chat through the sites the school allows

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

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

Appendix 1c - 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 ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the Online 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 ICT 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 Online 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 Online 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 Online Safety policy)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- I will only use my personal mobile ICT devices as agreed in the Online 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 ICT 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 ICT equipment in school, but also applies to my use of school ICT 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 ICT systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

Appendix 1d (From Herefordshire safety policy template) - Acceptable use agreement and permission forms – parent / carer

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

- that young people will be responsible users and stay safe while using ICT (especially the internet).
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of Online 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 ICT 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.

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 ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.

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

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

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

Parent's signature:	
Date:	

-
- **Use of digital images (still and video) of children**

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.

Images may also be used to celebrate success through their publication in newsletters, on the school website and in school controlled social media. The school will comply with the Data Protection Act and we will ensure that, when images are published, young people cannot be identified by name.

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

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, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images

Parent's signature:	
Date:	

I agree to images / video of my child being taken and used by approved 3rd party organisations (e.g. local newspapers, TV, radio) and I understand that these organisations may not adhere to our school code of practice (e.g. with respect to not printing names etc. alongside pictures)

Parent's signature:	
Date:	

- **Use of cloud based systems – permission form**

We are increasingly making use of mobile technology (iPads and other tables) in the course of learning in our school. These devices are bringing a whole new dimension to the use of technology in learning and bring completely new experiences to the children. Many of the apps we use (apps which are used across the world in schools) make use of cloud storage. The school strives for compliance with the data protection act in all respects here (for example we use Microsoft's One Drive as a means of sharing files between devices because their servers are located within the EU). We use only whole school or class accounts where cloud systems are involved and teachers talk regularly with children about the concept and safety of cloud based systems when these are used.

We ask for your consent to your child making use of this technology

Parent's signature:	
Date:	

- **Permission to publish children'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 and in the school's Remote Learning Environments (Seesaw etc)

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

Parent's signature:	
Date:	

Our school's Online 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.

Appendix 1e - Acceptable use policy agreement – community user

You have asked to make use of our school's ICT 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 ICT 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 ICT 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 ICT 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 ICT 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 Online 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

Sample Templates for incident recording / reporting in school

Sample Online Safety incident log form

Details of ALL Online Safety incidents are to be recorded by the Child Welfare Officer. This incident log will be monitored termly by Head teachers, Assistant Heads and Online Safety co-ordinator. Any incidents involving Cyber bullying should be recorded on the 'Integrated bullying and racist incident record Form'.

Date & Time	Name of pupil or staff member	Male or female	Room and computer device number	Detail of incident & evidence	Actions & reasons

Sample incident report form

Name of person	Name of Victim
Who reported the incident	Were parents informed
Witnesses	Parents response
Where incident took place	
Date(s) of incident(s)	
Description of incident(s)	
Resulting Actions/Follow up (if needed)	

Incident log completed by:

Date:

Weblinks

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/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 Online Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-Online-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 Online 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)