Kington Primary School

Online Safety Policy

Our School Vision

Developing caring, confident and creative children who achieve excellence.

Approved by:	Governors and Staff	**Date:**	May 2020
Last reviewed on:	September 2024		
Next review due by:	September 2025		

Contents

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. Children are generally much more open to developing technologies than many adults. 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
- 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 technology 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 technology.

A.1.1 Responsibilities: the online safety committee

The school council regularly discusses issues relating to online safety and when appropriate the staff representatives ask our Computing Lead or Designated Safeguarding Leads to attend its meetings. 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 Designated Safeguarding Team and Senior Management Team are people responsible to the head teacher and governors for the day to day issues relating to online safety. This team:

- leads discussions on online safety with the School Council where appropriate
- 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 school IT technical staff
- along with the DSL, receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- attends relevant meetings and committees of Governing Body
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

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 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:

- regular meetings with the DSL / SLT 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)

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 Computing Lead, DSL and SLT.
- 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 or DSL
- digital communications with students (using class email) 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: IT technician

Our ICT support is provided by D&D Network Services Ltd. The IT 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 computing coordinator or head teacher so that appropriate action may be taken.
- has responsibility for blocking / unblocking internet sites in the school's filtering system (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.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 and Support Staff

- Technical staff
- Governors (especially the online safety governor)
- Parents and Carers
- Pupils via the School Council

Schedule for development / monitoring / review of this policy

This online safety policy was approved by the governing body on:	*September 2020*
The implementation of this online safety policy will be monitored by the:	*The Computing Lead / SLT*
Monitoring will take place at regular intervals:	*Annually*
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:	*Annually*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments or online safety or incidents. The next anticipated review date will be:	*September 2024*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Hereford Safeguarding Children Board online safety representative* *Herefordshire Police / CEOP*

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 IT 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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate 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 IT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign.

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 IT systems)
- Community users of the school's IT system

Acceptable use policies are signed by all children as they enter school.

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments. Discussions with the children take place at the time.

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 a variety of permissions. 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 IT 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 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 IT / computing policies

Computing Policy - How computing / technology is used, taught, managed, resourced and supported in our school

Data Protection 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 and SMSC - online safety has links to this – staying safe

Safeguarding and Child Protection - Safeguarding children electronically is an important aspect of online safety. The online safety policy forms a part of the school's safeguarding policy and training, as does our Prevent training.

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 **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally, the following activities are also considered unacceptable on ICT 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 (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- 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	✓	✓	✓		✓	✓	✓	✓	

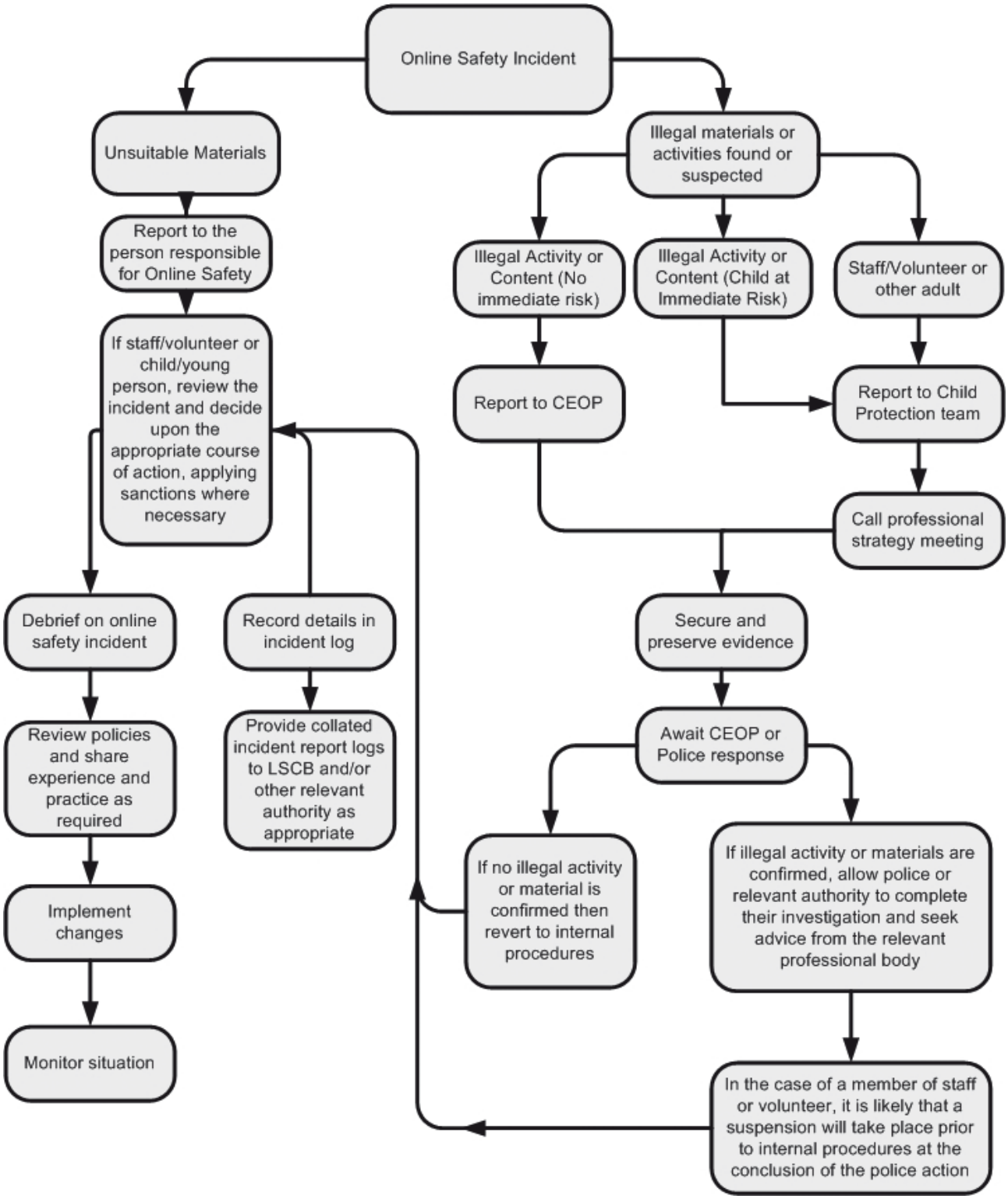
Staff sanctions

	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 e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓			✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓			✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with 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 technology, 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 head teacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

Mrs E.Bretherton – Headteacher/DSL , Mrs A.Welson – Deputy Headteacher/DDSL and Ms A.Deans – SLT/DDSL

The head teacher 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 head teacher 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

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

Further arrangements will be put in place to support pupils and staff who may have found some content distressing to deal with.

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 Mobile Technology (tablets, phones etc)

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

- It is not permissible for children to have access to staff tablets unless very carefully supervised.
- Members of staff are provided with gift cards to facilitate the purchase of apps for evaluation.
- A passcode is used on dedicated staff tablets (ensuring appropriate encryption of the device).
- 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.
- Members of staff are encouraged 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 but they should be kept away from pupils.
- Personal mobile devices should be used in lesson time only in an emergency or extreme circumstances.
- Members of staff are able to use these devices in school as long as it is reasonably away from pupils and outside teaching time.
- A school mobile phone is available for all professional use (for example when engaging in off-site activities) and members of staff should not use their personal device for school purposes except in an emergency.
- Any staff mobile technology brought into school must be protected with a PIN code.
- Members of staff are not permitted to 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 should 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.
- 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 normal filtering systems, while being used on the premises.
- All personal devices used in school must be passcode protected.
- Pupils receive training and guidance on the use of personal devices as part of their online safety education.

A.3.1c – School Owned devices used by pupils

- A growing number of tablets are available for children to use in school
- iPads are managed locally by the Computing Lead alongside D&D technicians.
- Age appropriate apps are purchased via Apple's VPP store and deployed with due regard to licensing and copyright.
- Files are transferred to / from and between iPads using carefully selected cloud storage solutions (One Drive) or Apple compatible USB drives.
- Parents give their general permission for use of class based cloud storage systems. Where individual pupil accounts are setup AND the data stored off site is open-ended or sensitive then specific permission is gained from parents (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:

- Where pupils bring mobile phones to school by prior agreement (between school and parents) 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 school server based email is provided for all users in school via the intranet page accessible via the web browser from their desktop.

In addition messaging (and email for staff) is available through other cloud based systems.

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

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications will 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.
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use. Google Classroom is also used as a form of communication between teachers and pupils.
- 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 communication.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

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

- Teachers are encouraged to use educationally sound social networking tools, e.g. blogging, with children
- Only approved tools are used
- The use of non-educational and age inappropriate social networking by children is forbidden.

A.3.2c - Videoconferencing

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.

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. See also section 3.1 for guidance on type of device used to capture / store images. The list of pupils who are not allowed to be pictured on the website is kept centrally in the school office.

- 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
- 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 in 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 the digital / video images.
- It is our school's policy to include a note to this effect on programmes or announcements during school performances, sporting events etc.

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 our website for sharing information with the community beyond our school. This includes celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- 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 or Facebook (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 – Cloud based systems

Class teachers monitor the use of cloud based systems by pupils regularly in all areas, but with particular regard to messaging and communication.

Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have accounts.

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.

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 a member of staff if the user does not comply.

c) Access to the system for the user may be suspended.

d) A pupil's parent/carer may be informed.

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, website 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, or ex-pupils (under the age of 18) as friends when personally using social networking sites.
- Staff members are strongly advised not to have parents as friends when personally using social networking sites.
- Staff members must not post comments / images / opinions that relate to school life.

Our whole school community constantly monitors and evaluates developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

Section B. Infrastructure

B.1 Password security

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

- users can only access data to which they have right of access.
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy.
- logs are maintained of access by users and of their actions while users of the system.

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email.

B.1.1 Policy Statements

All users (at KS2 and above) will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the Online safety Committee.

All users (at KS2 and above) will be provided with a username and password by the school's ICT Technician who will keep an up to date record of users and their usernames and has the ability to reset passwords.

Pupils in EYFS and KS1 do not usually use their individual logins, simple generic logins are used instead (though every pupil's individual login is available and ready to be used at any time and children in Y2 especially are often moved on when it is felt they are ready for this).

Users are not routinely required to change their passwords, though the school's online safety education programme makes clear the advantages of doing so and especially where high security is important. Users are required to change their passwords themselves if their details become known by another person. Class passwords (below KS2) are not changed.

Staff users have the facility to access all pupil work areas via their normal login. This is to enable monitoring of work and ICT activity by children.

This is also useful in the situation where a pair or group of children have been working collaboratively and the child whose login was used is unexpectedly absent; the teacher can move the work in question to another child's work area. In this way it is not necessary for a child to login using another child's account.

A multi-user account is available for visitors to the school (e.g. supply teachers). This has been carefully controlled to give only the access to the system that is needed and the username and password is given to users as required.

In the extraordinary case of a member of the wider community needing access to the school's ICT system outside the normal work of the school (e.g. for out of hours use by a community group) a special login is created by the school's ICT Technician with access rights agreed with the head teacher, ICT coordinator or online safety coordinator. Such users are required to sign an Acceptable Use Policy (see Appendix 1) before being granted this access.

Encryption software is installed on all staff laptops (where potentially sensitive data is stored and the machines are regularly taken off site).

The "master / administrator" passwords for the school ICT system used by the Network Manager and usually also the ICT coordinator must also be available to the head teacher or other nominated

senior leader and kept in a secure place (e.g. school safe). (Alternatively, where the system allows more than one "master / administrator" log-on, the head teacher or other nominated senior leader should be allocated those master / administrator rights. A school should never allow one user to have sole administrator access).

B.1.2 Responsibilities

The ICT technician will be responsible for the day to day management of the password security policy

All users (adults and young people other than pupils in EYFS and KS1) will have responsibility for the security of their username and password. They:

- must not allow other users to access the systems using their log on details and
- must immediately report any suspicion or evidence that there has been a breach of security
- must change their password if they are aware that it has become known by another user.
- must logoff at the end of their session or lock the screen (Windows + L) before leaving the computer.

EYFS and KS1 pupils use class logins which are shared.

Passwords for new users, and replacement passwords for existing users can be allocated by the ICT technician or, if needed more immediately, the ICT coordinator.

B.1.3 Training and awareness raising

We recognise that is important that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. Please see section for specific guidance on e-safety education (which includes the use of passwords)

Members of staff will be made aware of the school's policy on the use of passwords:

- at induction
- through this policy
- through the Acceptable Use Agreement (see Appendix 1)

Pupils will be made aware of the school's policy on the use of passwords:

- in ICT and / or online safety lessons (the school should describe how this will take place)
- through the Acceptable Use Agreement (see Appendix 1)

B.1.4 Audit, monitoring, reporting and review of password policy

The Computing Coordinator and IT Technician will ensure that full records are kept of:

- User IDs and requests for password changes
- User logins
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

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 (this section) to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Our school buys broadband services through D&D and 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 headteacher and SLT (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 filtering service must:

- be logged in change control logs
- be reported to a second responsible person *(the head teacher / computing coordinator)* within the time frame stated in section A.1.3 of this policy
- If staff feel a website should not be filtered / blocked, they are to make this known to the computing coordinator. The computing coordinator will then assess the site themselves before making a request to D&D network solutions.
- **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.
- The online safety coordinator will need to apply a rigorous policy for approving / rejecting filtering requests. This can be found in Appendix 3 but the core of this should be based on the site's content:
- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.

B.2.1c - 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).
- Being vigilant in lessons and monitoring closely the pupils' access and activities online on school devices.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through online safety awareness sessions / newsletter etc.

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

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

- The teacher makes the request to D&D, via the Computing Lead or the School Administrator.
- D&D checks the website content to ensure that it is appropriate for use in school.
- D&D helpdesk will endeavour to unblock the site 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.

B.2.1e – Monitoring, auditing and reporting

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

- Logs of filtering change controls and of filtering incidents are made available to
  - the online safety coordinator and/or 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.3 Technical security

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in this policy and acceptable use policy.
- There will be regular reviews and audits of the safety and security of school systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

The school infrastructure and individual workstations are protected by up to date virus software.

Pupil accounts allow access to limited storage areas; they cannot access local hard drives and are unable to run executable files.

Staff accounts allow greater access to the network and to local drives. Staff are able to run executable files but do so within the acceptable use agreement they sign (see Appendix 1)

Staff laptops and mobile devices can be provided for staff professional use while the member of staff is employed by the school.

- These machines are allowed off-site and are protected by encryption software where sensitive data is stored
- Members of staff are permitted to install software and apps on this equipment as long as the installation is legal, within the scope of the licensing agreement owned by the school and professionally necessary.
- The storage of personal files (including image, music and video collections) on computers owned by the school is not permitted.
- Members of staff are not permitted to store school data on personally owned devices.

Please refer to the sections in A.3 of the online safety policy for further guidance on acceptable use.

B.3.1 Personal data security (and transfer)

This is dealt with in detail in our school's ***Data 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 Computing, PHSE and other lessons and should be regularly revisited – this will cover the use technology in school and outside school
- We use resources from numerous sites / companies to support Online Safety, such as (Parent Zone, Google: Be Internet Legends, Twinkl, Safer Internet Day in February of each year).
- Learning opportunities for online safety are built into the Computing Policy progression of teaching.
- 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 technology 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 freely to search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Staff undertake PREVENT training regularly as part of our Safeguarding training programme.

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.

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 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 online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- The school constantly monitors staff training needs and a programme of online safety training will be made available to staff.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should ensure 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 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.

C.3 Governor training

Governors should take part in online safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the local authority, national or local 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, website,
- Parents evenings
- Referring parent to a range of online resources (saferinternet.org.uk, internetmatters.org, Wake Up Wednesday online safety guides)

C.5 Wider school community understanding

The school may from time to time offer family learning courses in IT, 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.

Community Users who access school IT systems 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 1 – Acceptable use policy agreement templates

The following pages contain Acceptable Use Agreements for:

- EYFS and Key Stage 1 Pupils (Three Cs for Computers)
- Key Stage 2 Pupils (Our School's Three Cs of online Responsibility)
- Key Stage 2 Pupils (more formal version)
- Parents and Carers
- Staff and Volunteers
- Community User of the school's ICT facilities

Three Cs for Computers (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

Our 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

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

For my professional and personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (laptops, tablets, email, cloud based technologies etc) out of school.
- I understand that the school IT 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 an appropriate person.

I will be professional in my communications and actions when using school IT 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) it will not be possible to identify by full 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 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.
- I will not have pupils, or ex-pupils (under the age of 18) as friends when personally using social networking sites.
- I understand that I am strongly advised not to have parents when personally using social networking sites.
- I understand that I must also not post comments / images that relate to school life when personally using social networking sites.

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 IT 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. I will not use my mobile phone when there are children present in the room.
- I will not open any attachments to emails, unless the source is known and trusted.
- 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 applications that might allow me to bypass the filtering / security systems.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where personal data is transferred outside the secure school network I understand that 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.

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 IT equipment in school, but also applies to my use of school IT 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 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 - 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 eceive, online safety education to help them understand the importance of safe use of technology – 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 IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed.

I understand that my son's / daughter's activity on the IT 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 devices 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 their full 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. To respect everyone's privacy (and in some cases protection) these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other 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 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 new experiences to the children. Many of the apps we use make use of cloud storage. The school strives for compliance with the data protection act in all respects here. Where class / school based systems are used we ask for your permission here. In the case of cloud based systems where individual pupil accounts are created AND the nature of the data stored there is open ended or sensitive we will seek your permission on an individual basis when we consider this to be necessary. 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 cloud based storage systems.

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 - 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 the Headteacher, Deputy Headteacher 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:

Appendix 3 - Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
DfE	Department for Education
FOSI	Family online Safety Institute
HSCB	Herefordshire Safeguarding Children Board (the local safeguarding board)
ICT	Information and Communications Technology
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 (e.g. 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
PHSE	Personal, Health and Social Education
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)