Leominster Primary School

E-safety Policy

Contents

Background and rationale .....

Section A - Policy and leadership .....

A.1.1 Responsibilities: the e-safety committee.....

A.1.2 Responsibilities: e-safety coordinator.....

A.1.3 Responsibilities: governors .....

A.1.4 Responsibilities: head teacher .....

A.1.5 Responsibilities: classroom based staff.....

A.1.6 Responsibilities: ICT technician .....

A.2.1 Policy development, monitoring and review .....

Schedule for development / monitoring / review of this policy .....

A.2.2 Policy Scope.....

A.2.3 Acceptable Use Policies.....

A.2.4 Self Evaluation.....

A.2.5 Whole School approach and links to other policies.....

Core ICT policies .....

Other policies relating to e-safety.....

A.2.6 Illegal or inappropriate activities and related sanctions.....

A.2.7 Reporting of e-safety breaches .....

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

Responsibilities.....

Training / Awareness.....

Our search policy.....

Electronic devices.....

Deletion of Data .....

Audit / Monitoring / Reporting / Review .....

A.3.1 Use of hand held technology (personal phones and hand held devices) .....

A.3.2 Use of communication technologies.....

A.3.2a - Email.....

A.3.2b - Social networking (including chat, instant messaging, blogging etc) .....
A.3.2c - Videoconferencing .....
A.3.3 Use of digital and video images .....
A.3.4 Use of web-based publication tools .....
A.3.4a - Website (and other public facing communications) .....
A.3.4b - Virtual Learning Environment (VLE) .....
A.3.5 Professional standards for staff communication .....
Section B. Infrastructure .....
B.1 Password security .....
B.2.1 Filtering .....
B.2.2 Technical security .....
B.2.3 Personal data security (and transfer) .....
Section C. Education .....
C.1.1 E-safety education .....
C.1.2 Information literacy .....
C.1.3 The contribution of the children to e-learning strategy .....
C.2 Staff training .....
C.3 Governor training .....
C.4 Parent and carer awareness raising .....
C.5 Wider school community understanding .....
Appendix 1 – Acceptable use policy agreement templates .....
Appendix 1a – Acceptable use policy agreement – pupil (KS1) .....
Appendix 1b – Acceptable use policy agreement – pupil (KS2) .....
Appendix 1c - Acceptable use policy agreement – staff & volunteer .....
Appendix 1d - Acceptable use policy agreement and permission forms – parent / carer .....
Appendix 1e - Acceptable use policy agreement – community user .....
Appendix 1f - Acceptable use policy agreement - I pad at home for staff and volunteer
Appendix 2 - Guidance for Reviewing Internet Sites .....
Appendix 3 – Criteria for website filtering .....
Appendix 4 - Supporting resources and links .....
Sample Templates for incident recording / reporting in school .....
Appendix 5 - Glossary of terms .....

Background and Rationale

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

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

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.

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

Our school's e-safeguarding policy has been written from a template provided by Herefordshire Council's Learning and Achievement Service which has itself been derived from that provided by the South West Grid for Learning.

Section A - Policy and Leadership

This section begins with an outline of the **key people responsible** for developing our E-Safety Policy and keeping everyone safe with 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 e-safety committee

The school council regularly discusses issues relating to e-safety and when appropriate the staff representatives ask our school e-safety coordinator 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: e-safety coordinator

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

- leads discussions on e-safety with the School Council
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly (once a year) with e-safety governor to discuss current issues, review incident logs and filtering change control logs
- attends relevant meetings and committees of Governing Body
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively
- has responsibility for passing on requests for blocking / un blocking to the 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 e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor which involves:

- regular meetings with the E-Safety Co-ordinator (once a year) with an agenda based on:
- monitoring of e-safety incident logs
- monitoring of filtering change control logs
- monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices (see section A.2.8)
- reporting to relevant Governors committee / meeting

A.1.4 Responsibilities: head teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-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 e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in section 2.6 below and relevant Local Authority HR / disciplinary procedures)

A.1.5 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

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

A.1.6 Responsibilities: 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 e-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority E-Safety Policy and guidance
- users may only access the school's networks through a properly enforced password protection policy as outlined in section B.1 of this policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

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

- School E-Safety Coordinator
- Head teacher / Senior Leaders
- Teachers
- Governors (especially the e-safety governor)

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

- School Council
- INSET Day
- Governors meeting / subcommittee meeting

Schedule for development / monitoring / review of this policy

This e-safety policy was approved by the governing body on:	
The implementation of this e-safety policy will be monitored by the:	E-Safety Coordinator, Head Teacher, Senior Leadership Team and E-safety Governor.
Monitoring will take place at regular intervals:	Once a year
The governing body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Once a year
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	February 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Hereford Safeguarding Children Board e-safety representative Herefordshire Police

A.2.2 Policy Scope

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

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

A.2.3 Acceptable Use Policies

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

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

- Pupils (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.

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.

If parents/carers don't want their child's photograph to be taken or work to be displayed on the internet then they must sign and return a declaration to inform the school.

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

We have a system that logs information about unacceptable sites and expressions that are used on our school networks, for example: radicalisation, bullies and inappropriate content. This system is then monitored by a member of staff who will deal with any concerns from a pupil or member of staff.

A.2.4 Self Evaluation

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

A.2.5 Whole School approach and links to other policies

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

Core ICT policies

ICT Policy	How ICT is used, managed, resourced and supported in our school
E-Safety Policy	How we strive to ensure that all individuals in school stay safe while using ICT. The e-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 e-safety policy.
The Herefordshire ICT Progression	Four core age specific documents (and associated resources) directly relating to learning and covering the ICT Curriculum. See www.hereford-edu.org.uk/ict

Other policies relating to e-safety

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

A.2.6 Illegal or inappropriate activities and related sanctions

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

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

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

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

Additionally the following activities are also considered unacceptable on 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 e-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator for	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

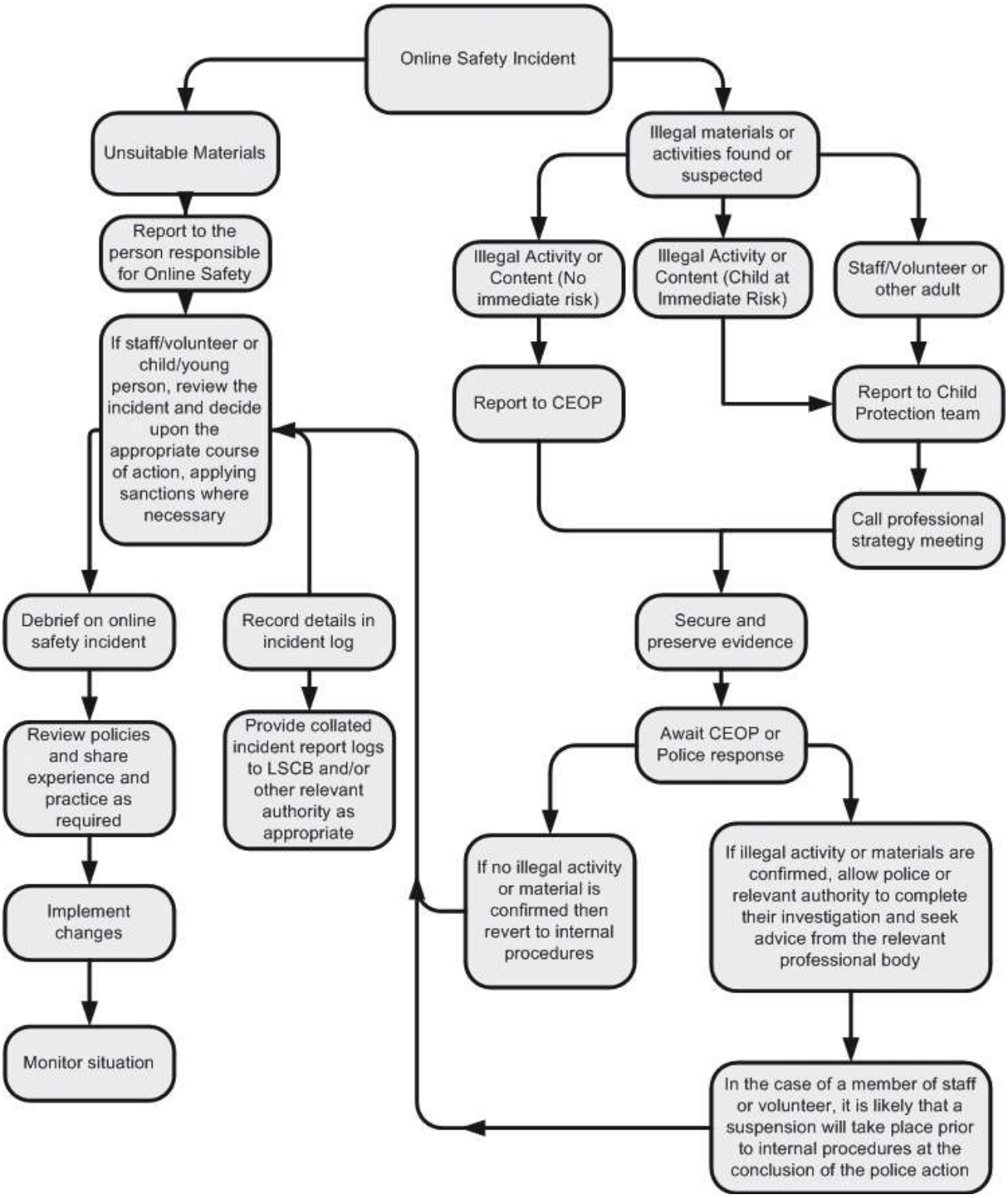
	Refer to line manager	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section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


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

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

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

Responsibilities

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

Training / Awareness

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

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

Our search policy

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

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

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

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

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

In carrying out the search:

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

Extent of the search:

- The person conducting the search may not require the pupil to remove any clothing other than outer clothing.
    - Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

- *A* pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.
    - 'Possessions' means any goods over which the pupil has or appears to have control – this includes 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 is kept of the reasons for the deletion of data / files.

Audit / Monitoring / Reporting / Review

The E-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.
    - A school mobile phone is available for all professional use (for example when engaging in off-site activities) and members of staff are also allowed to use their personal device for school purposes.

- Pupils are not currently permitted to bring their personal hand held devices into school except on specific occasions when advertised. If bought into school then children should hand them into the school office, where they are stored in a secure location.
- A number of such devices are available in school (e.g. ActivExpression, ActiVote, IPod) and are used by children as considered appropriate by members of staff.

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

A.3.2 Use of communication technologies

A.3.2a - Email

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

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

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

Use of Email	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
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)

Use of social networking tools	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
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.3.3 Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
- 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 the responsibility of parents when taking photographs within the school grounds. Staff request that parents only take photographs of their children and not to publish them on social networking sites.
- Each individual year group to have their own school camera. The use of staff personal cameras is at the head's discretion.

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 (www.OurSchoolName.hereford.sch.uk) 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, and only then when necessary.
- Detailed calendars are not published on the school website. Password protected areas of website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

A.3.4b - Virtual Learning Environment (VLE)

Currently not applicable.

A.3.5 Professional standards for staff communication

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

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

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

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

Section B. Infrastructure

B.1 Password security

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)

Supply teachers have specific supply accounts in order to gain access to the network. These passwords are changed regularly.

By the end of Key Stage 2, pupils should have individual passwords to log on to laptops.

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 **e-safety coordinator** (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

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

- be logged in change control logs
- be reported to a second responsible person (the head teacher / ICT coordinator [if they are not also the e-safety coordinator] / e-safety governor) within the time frame stated in section A.1.3 of this policy
- be authorised by a second responsible person prior to changes being made.

All users have a responsibility to report immediately to class teachers / e-safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

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

B.2.1c - Education / training / awareness

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

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

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

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

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

One filtering policy, primarily designed for the purpose of pupil internet access, is in use in our school. This policy applies to all users in many primary schools.

Changes (if agreed) are made on request by ICT Services and reviewed by the LA ICT consultants.

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

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

- If agreement is reached, the e-safety coordinator logs the request with the Schools ICT Helpdesk on 01432 261500 or schoolshelpdesk@herefordshire.gov.uk
- The schools helpdesk will endeavour to unblock the site at the time of the call 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 schoolboy the e-safety coordinator or requested of the Herefordshire ICT Schools Helpdesk.

B.2.1f - Audit / reporting

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

- the e-safety governor within the timeframe stated in section A.1.3 of this policy
- the 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 E-safety education

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

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

- A planned e-safety programme should be provided as part of 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 on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)

- Learning opportunities for e-safety are built into the *Knowledge and Understanding* sections of the *Herefordshire Primary ICT Progression* where appropriate and are used by teachers to inform teaching plans. (www.hereford-edu.org.uk/ict)
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

C.1.2 Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
    - Checking the likely validity of the URL (web address)
    - Cross checking references (can they find the same information on other sites)
    - Checking the pedigree of the compilers / owners of the website
    - See lesson 5 of the Cyber Café Think U Know materials below
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)

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

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

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

C.2 Staff training

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

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

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

C.3 Governor training

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

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

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

C.4 Parent and carer awareness raising

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

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

- Letters/newsletters
- Web site
- Parents evenings

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

	• I will always keep my passwords a secret • I will always keep my personal details (name, family information, journey to school, pets and hobbies) private.
	• I will only open pages which my teacher said are ok. • I will talk to my teacher before using anything on the internet. • I will tell a teacher or my parents if I see anything that that makes me uncomfortable or scared when online.
	• I will make sure all messages are or emails are polite. • I will only email or message people I know or if my teacher agrees.
	• I will only work with people I know in real life. • I will make sure all messages I send are polite. • I will tell a teacher or my parents if I receive a nasty message. • I will not reply to any nasty messages. • I will never agree to meet a stranger. • I will not load photographs of myself onto the computer.
	• I will look after school computing equipment and tell a teacher straight away if something is not working or broken.
	• I will not give my mobile phone number to anyone who is not a friend in real life.

I will always use what I have learned about e-safety to keep myself safe online.

Name: _____ Date: _____

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

	• I will only use my own username and password • I will always keep my passwords a secret • I will always keep my personal details (name, family information, journey to school, pets and hobbies) private. • I will not try to get past any security measures in place to protect the school network
	• I will only visit sites that are appropriate to my work at the time. • I will tell a responsible adult if I see anything that makes me worried or uncomfortable when online.
	• I will only use my school email account. • I will make sure all emails I send are respectful. • I will only open any email attachment when approved by an adult. • I will only email or message people I know or those approved by a responsible adult.
	• I will make sure all messages I send are respectful. • I will tell a responsible adult if I receive messages that make me worried or uncomfortable when online. • I will not reply any nasty messages or things that make me feel uncomfortable. • I will only send messages to people I know or those approved by a responsible adult. • I will talk to a responsible adult before joining chat rooms or networking sites. • I will never meet an online friend without taking a responsible adult that I know with me. • I will always check with a responsible adult before I share photographs of myself.
	• I will use ICT equipment safely and responsibly. • I will only use school ICT equipment for my work. • I will make sure all my work doesn't break copyright rules.
	• I will not give my mobile phone number to anyone who is not a friend in real life. • I will always check with a responsible adult before I share photographs of myself.

I will always use what I have learned about e-safety to keep myself safe online.

Name: _____ Date: _____

Appendix 1c - Acceptable use policy agreement – staff & volunteer

LEOMINSTER PRIMARY SCHOOL

STAFF ACCEPTABLE USE OF INTERNET AND NETWORK

School Employee's Agreement:

I understand that access to the Internet from Leominster Primary School (LPS) must be in support of educational activities, research or learning. I accept that private use of the Internet in school is forbidden and this includes playing E-games or entering chat rooms. I agree to the following:

1. I understand that the school monitors real time usage of the Internet; keeps a record of when I use it; and keeps an electronic log of which sites I visit or attempt to visit.
2. I will not access any areas of the Internet that are inappropriate or offensive. This applies to any material of an illegal, illicit, violent, dangerous, racist or sexual content.
3. I will take responsibility for checking and rejecting inappropriate or offensive information, which I receive or access and will inform the Computing Co-ordinator and/or IT Technician, which need to be filtered.
4. I will not disclose any password or login name, including SIMS passwords, to anyone, other than the persons responsible for running and maintaining the system.
5. I will not give personal information including credit card numbers, postal or email addresses, telephone or fax numbers, or use photographs of any pupils or other adults at the school.
6. I will not use names or photographs of pupils without the written permission of their parents/ guardians.
7. I accept responsibility to keep copyrighted material from entering the school. Therefore, I will not download any software, games, music, graphics, videos or text materials that are copyrighted.
8. I will always respect the privacy of files of other users. I will not enter the file areas of other school employees without their permission.
9. I will be polite and use appropriate language in all my computing communications. I will not state anything, which could be interpreted as libel.
10. I will arrange for appropriate suitable monitoring of any pupils to whom I have given permission to use the Internet facilities.
11. I will report any incident, which breaches the Acceptable Rules Policy immediately to the computing Co-ordinator or the Headteacher.
12. I understand that I am responsible for making sure that I lock my PC, if I leave it unattended.
13. I understand that if I do not lock my PC when leaving it unattended, I will be held responsible for any data protection issues that may occur.
14. I will use an LPS encrypted memory stick when moving data between locations.
15. I will change my password every half term. It will include upper and lower case letters, numbers and at least one wild card (e.g. an exclamation mark, star, question mark, etc.).
16. My SIMS password and network passwords will be different.
17. I will only use my school laptop at home if I am logged into the VPN and saving to the F: drive.
18. I will ensure I do not save passwords to my computer or use automatic log in for the VPN.
19. I will use an LPS encrypted memory stick when moving data between locations.

I understand and agree to maintain all the above rules whenever I use the School's computing equipment.

Employee's name :……(please print)

Signed:…… Date:……

Appendix 1f - Acceptable use policy agreement – staff & volunteer

LEOMINSTER PRIMARY SCHOOL

STAFF ACCEPTABLE USE OF an IPad at home

School Employee's Agreement:

I understand that access to the Internet from Leominster Primary School devices (LPS) must be in support of educational activities, research or learning. I accept that private use of the Internet using an IPad is forbidden and this includes playing E-games or entering chat rooms. I agree to the following:

20. I understand that the only use of the device is to upload data and photos to Tapestry.
21. I will not disclose any password or login name, including SIMS passwords, to anyone, other than the persons responsible for running and maintaining the system.
22. I will not give personal information including credit card numbers, postal or email addresses, telephone or fax numbers, or use photographs of any pupils or other adults at the school except when uploading data to Tapestry.
23. I will delete all photos off the IPad once they have been uploaded to Tapestry.
24. I will not use names or photographs of pupils without the written permission of their parents/ guardians.
25. I will be polite and use appropriate language in all my computing communications. I will not state anything, which could be interpreted as libel.
26. I will report any incident, which breaches the Acceptable Rules Policy/ data protection policy immediately to the computing Co-ordinator or the Headteacher.
27. I understand that I am responsible for making sure that I lock my IPad, if I leave it unattended.
28. I understand that if I do not lock my IPad when leaving it unattended, I will be held responsible for any data protection issues that may occur.
29. I will be the only person who accesses the IPad outside of school.
30. It is my responsibility to ensure that the IPad is kept in a secure place at all times.
31. I must not use public available storage such as drop box or Google drive to store any school data.
32. I will change my password every half term. It will include upper and lower case letters, numbers and at least one wild card (e.g. an exclamation mark, star, question mark, etc.).
33. I accept responsibility for keeping all data on the IPad secure and making sure that I comply with the schools data protection policy at all times. I also understand that I am only to use the IPad to access Tapestry.

I understand and agree to maintain all the above rules whenever I use the School's computing equipment.

Employee's name :……(please print)

Signed:…… Date:……

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

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

Consent Form for Photography and Images of Children

Dear Parent or Guardian

During your child's life at Leominster Junior School we may wish to take photographs of activities that involve your child. The photographs may be used for displays, publications and on a website by us, by the Local Authority (LA) or by local newspapers.

Photography or filming will only take place with the permission of the Headteacher, and under appropriate supervision. When filming or photography is carried out by the news media, children may be named but home addresses will never be given out. Images that might cause embarrassment or distress will not be used nor will images be associated with material on issues that are sensitive.

Before taking any photographs of your child, we need your permission. ***Please answer the questions below, sign and date the form and return it to us.*** You can ask to see images of your child held by us. You may withdraw your consent, in writing, at any time.

<table>
<tr><td colspan="2">Name of child (Block Capitals):</td><td></td></tr>
<tr><td colspan="2">Name of person responsible for the child:</td><td></td></tr>
<tr><td colspan="3">I understand that:
The local media may take images of activities that show the school and children in a positive light e.g. Reception Year pictures of new starters, drama and musical performances, sports and prize giving
Photographers acting on behalf of the school or the LA may take images for use in displays, in publications or on a website
Embarrassing or distressing images will not be used
The images will not be associated with distressing or sensitive issues
The school will regularly review and delete unwanted material.</td></tr>
<tr><td rowspan="3">Having read the above statement, do you give your consent for photographs and other images to be taken and used?
(please tick the appropriate box/boxes)

The term "published" refers to being used on the school or local authority websites or in the media.</td><td></td><td>YES, I give my consent for pictures to be taken and used within the school but not to be used in the press or on the school websites.</td></tr>
<tr><td></td><td>YES, I give my consent for pictures of my child to be published, with their names and ages, in the press or on the school, Local Authority or press websites.</td></tr>
<tr><td></td><td>YES, I give my consent for pictures of my child to be published in the press or</td></tr>
</table>

		on the school, Local Authority or press websites but not for them to be named.
		NO, I do not give my permission for pictures to be taken and used inside or outside the school
Signature of person responsible for the child:		
Relationship to the child:		
Date (Date/Month/Year):		

NB. There may be other circumstances, falling outside the normal day to day activities of the school, in which pictures of children are requested. The school recognises that in such circumstances specific consent from parent or guardian will be required before photography or filming of children can be permitted.

If you wish to attend school functions and take photographs of your and other people's children please take appropriate images, be sensitive to other people and try not to interrupt or disrupt concerts, performance and events. Thank you.

Appendix 2 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse3 then the monitoring should be halted and referred to the Police immediately4. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

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

Appendix 3 – Criteria for website filtering

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors (about us, our objectives, etc.)
- There is a contact for further information and questions concerning the site's information and content.

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

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

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

- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for the pupils
- Is the website current?

D. ACCESSIBILITY - Is the website accessible?

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

Appendix 4 - Supporting resources and links

Templates for incident recording / reporting in school

E-safety incident log form

Details of ALL e-safety incidents are to be recorded by the Child Welfare Officer. This incident log will be monitored termly by Head teachers, Assistant Heads and E-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

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 5 - Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are still used)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
DfE	Department for Education
FOSI	Family Online Safety Institute
HSCB	Herefordshire Safeguarding Children Board (the local safeguarding board)
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by Becta
ICT Services	Herefordshire ICT Services - provide broadband services and ICT support to Herefordshire schools
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
KS1 ..	KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)
LA	Local Authority
LAN	Local Area Network
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
SRF	Self Review Framework – a tool maintained by Naace used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to e-safety (on whose policy this one is based)
URL	Universal Resource Locator – posh name for a web address
VLE	Virtual Learning Environment - an online system designed to support teaching and learning in an educational setting,

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

Staff Responsible: IT Coordinator

Date of Review: Summer 2017

Date of Next Review: Summer 2019

Ratified by Governors 14th July 2017