Herefordshire Computing Support – Learning and Achievement Service

E-Safety Policy for Madley Primary School

This document can be downloaded from www.herefordshirecomputing.com

Learning and Achievement Service
Herefordshire Computing Support
hands on learning and teaching

Introduction

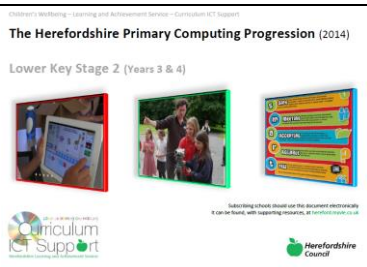
This Primary School E-Safety Policy Template is intended to help schools produce a suitable E-Safety policy document which will consider all current and relevant issues, in a whole school context, linking with other relevant policies. National guidance suggests that it is essential for schools to take a leading role in e-safety.

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> "One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

Schools are expected, by Ofsted, to evaluate their level of e-safety and are now subject to an increased level of scrutiny of all safeguarding issues during school inspections.

How to use this policy template

	**This template policy for Herefordshire schools** draws heavily on the template provided by the **South West Grid for Learning**; internationally recognised as a leading authority on all matters relating to e-safety. The template has been adapted in the light of provision in Herefordshire and can form the basis of any Herefordshire school's own policy. The original SWGfL materials can be found at http://www.swgfl.org.uk/Staying-Safe
	The **e-security policy** is a sister policy template to this one which should be adapted and used alongside this e-safety policy. This second policy relates to the security of data and data systems in school as well as good practice around transfer of this data. Generally speaking this is good practice that underpins e-safety and this e-safety policy but which does not directly relate to the children in your school. You'll find this at www.herefordshirecomputing.com
	**The 360 Degree Safe E-Safety Mark** is a recognised award provided through SWGfL. The 360 Degree Safe self-review tool that leads to this award is free of charge and is an excellent way to evaluate your school's e-safety provision (perhaps alongside the adaptation and implementation of this policy). To help you further in this process, we have reorganised this policy template to reflect exactly the headings in the assessment tool. The statements contained in this policy, if transferred from policy to practice, will allow your school to meet the required standards for the 360 Degree Safe award. The self-review tool can be found at www.360degreesafe.org.uk
	E-safety education is a vital component of e-safety. You will find e-safety pointers in the digital literacy section of the **Herefordshire Primary Computing Progression.** This document outlines the knowledge skills and understanding that need to be taught throughout the primary phase and contains a complete range of readymade lessons, from a variety of excellent sources. These schemes of work can be found at www.herefordshirecomputing.com

How shall we go about writing our policy?

This is a key consideration. If it is to be effective your school's e-safety policy must be tailored to the needs of your school **and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy**. This will help ensure that the policy is owned and accepted by the whole school community. It is suggested that consultation in the production of this policy should involve senior leadership and governors, classroom based staff, pupils and parents.

A good way to go about this task might be to ask a member of the Herefordshire Computing Support team to come and lead a staff meeting at which we can modify this template to your needs and leave you with your own policy. This will have the advantage of involving all staff who will then be familiar with the issues involved. **This is an import issue as e-safety involves many concepts that are not immediately understood by all, and the session will also serve as an awareness raising and CPD opportunity.** If you choose to do this, it would be good to have representatives from all of the above groups involved with the process. Please contact msanderson@hereforsdshire.gov.uk to arrange a session in your school.

Practicalities – modifying the document

> Within this template sections which include information or guidance are shown in small print and in a box like this one. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Statements and bullet points in normal text are those that we consider should form a part of your finished policy, though feel free to modify them so that they reflect your approach in school.

Where sections in the template are written *in italics* you should consider whether or not to include that statement (or a modified version of it) in your policy.

To update the table of contents just right click over any part of it and select *Update Field* then choose *Update entire table.*

Links to other core computing policies

You will have other core computing policies in school (if not, Herefordshire templates are available for those too) and it is important that these all agree. We suggest the following:

Computing Policy	How technology 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 technology. The e-safety policy constitutes a part of the computing policy. (This policy)
E-Security Policy	How we categorise, store and transfer sensitive and personal data. This links strongly and overlaps with the e-safety policy.
Computing Progression	Three key documents and associated resources directly relating to learning covering the computing curriculum (2014)

Links to other policies relating to e-safety

There are obvious links to other policies that will exist in school and again it is import that they are in line with each other. You may wish to visit the following to check this: Anti-bullying, PSHE, Safeguarding, Behaviour

Wider consultation

In producing this template policy we have worked with other local organisations, in particular:

- The Herefordshire Safeguarding Children Board (HSCB)
- Providers of technical support for Herefordshire schools
- Policy documents from other local authorities and RBCs, in particular SWGfL and Kent County Council

Mark Sanderson – Herefordshire Learning and Achievement Service - February 2016

Contents

Introduction 3

How to use this policy template 3

Contents 5

Background and rationale 7

Section A - Policy and leadership 8

A.1.1 Responsibilities: the e-safety committee 8

A.1.2 Responsibilities: e-safety coordinator 8

A.1.3 Responsibilities: governors 9

A.1.4 Responsibilities: head teacher 9

A.1.5 Responsibilities: classroom based staff 9

A.1.6 Responsibilities: IT technician 9

A.2.1 Policy development, monitoring and review 10

Schedule for development / monitoring / review of this policy 10

A.2.2 Policy Scope 10

A.2.3 Acceptable Use Policies 11

A.2.4 Self Evaluation 11

A.2.5 Whole School approach and links to other policies 11

Core IT / computing policies 11

Other policies relating to e-safety 11

A.2.6 Illegal or inappropriate activities 12

A.2.7 Reporting of e-safety breaches 13

A.2.8 Electronic Devices - Searching & Deletion (June 2012) 13

Training / Awareness 14

Our search policy 14

Electronic devices 15

Deletion of Data 15

Audit / Monitoring / Reporting / Review 15

A.3.1 Use of Mobile Technology (tablets, phones etc) 15

A.3.1a – School Owned devices allocated to members of staff 15

A.3.1b – Personally owned staff devices 16

A.3.1c – School Owned devices used by pupils 16

A.3.1d – Personally owned pupil devices 16

A.3.2 Use of communication technologies 16

A.3.2a – Email 16

A.3.2b - Social networking (including chat, instant messaging, blogging etc) 17

A.3.2c - Videoconferencing 17
A.3.3 Use of digital images (still and video) 17
A.3.4 Use of web-based publication tools 17
A.3.4a - Website (and other public facing communications) 17
A.3.4b – Cloud based systems 18
A.3.5 Professional standards for staff communication 18
Section B. Infrastructure 19
B.1 Password security 19
B.2.1 Filtering 19
Section C. Education 20
C.1.1 E-safety education 20
C.1.2 Information literacy 20
C.1.3 The contribution of the children to e-learning strategy 20
C.2 Staff training 21
C.3 Governor training 21
C.4 Parent and carer awareness raising 21
C.5 Wider school community understanding 21
Appendix 1 – Acceptable use policy agreement templates ..... **Error! Bookmark not defined.**
Three Cs for Computers (EYFS & KS1 AUP) ..... **Error! Bookmark not defined.**
Our School's Three Cs of Online Responsibility (KS2 AUP) ..... **Error! Bookmark not defined.**
Appendix 1b – More Formal Acceptable use policy agreement – pupil (KS2) ..... **Error! Bookmark not defined.**
Appendix 1c - Acceptable use policy agreement – staff & volunteer ..... **Error! Bookmark not defined.**
Appendix 1d - Acceptable use agreement and permission forms – parent / carer .. **Error! Bookmark not defined.**
Appendix 2 - Supporting resources and links ..... **Error! Bookmark not defined.**
Sample Templates for incident recording / reporting in school ..... **Error! Bookmark not defined.**
Appendix 3 - Glossary of terms ..... **Error! Bookmark not defined.**

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 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 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 e-safety committee

Our school has an e-safety committee led by our e-safety coordinator and made up of pupils, teachers and our safeguarding governor. It meets on a termly basis to

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

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

OR

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

> It is strongly recommended that each school should have a named member of staff with a day to day responsibility for e-safety; some schools may choose to combine this with the Child Protection Officer role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school and will very much depend on the size of the school as to who this person will be.

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 the e-safety committee and discussions on e-safety
- 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 school IT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-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
- 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 (agree time frame) with an agenda based on:
    - monitoring of e-safety incident logs
    - logs from Policy Central
    - 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 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: IT technician

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 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
- short comings in the infrastructure are reported to the computing coordinator or head teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

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

- *School E-Safety Coordinator*
- *Head teacher*
- *Governors*

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

- Staff meetings
- E-Safety assemblies
- Governors meeting / subcommittee meeting
- Parents evening
- School website / newsletters

Schedule for development / monitoring / review of this policy

This e-safety policy was approved by the governing body on:	Autumn term 17
The implementation of this e-safety policy will be monitored by the:	E-safety coordinator and /or Computing coordinator
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 or e-safety or incidents. The next anticipated review date will be:	Autumn term 18
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Hereford Safeguarding Children Board e-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 e-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 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 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 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.

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

A.2.4 Self Evaluation

Evaluation of e-safety is an on-going process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers and volunteers) 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, 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 computing policy.
E-Security Policy	How we categorise, store and transfer sensitive and personal data. This links strongly and overlaps with this e-safety policy.
Herefordshire Computing Progression	Three core age specific documents (and associated resources) directly relating to learning and covering the computing curriculum.

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
PREVENT	Included in our safeguarding policy. This is an online training session which all staff, volunteers and practitioners complete on an annual basis
Behaviour	Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

A.2.6 Illegal or inappropriate activities

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.

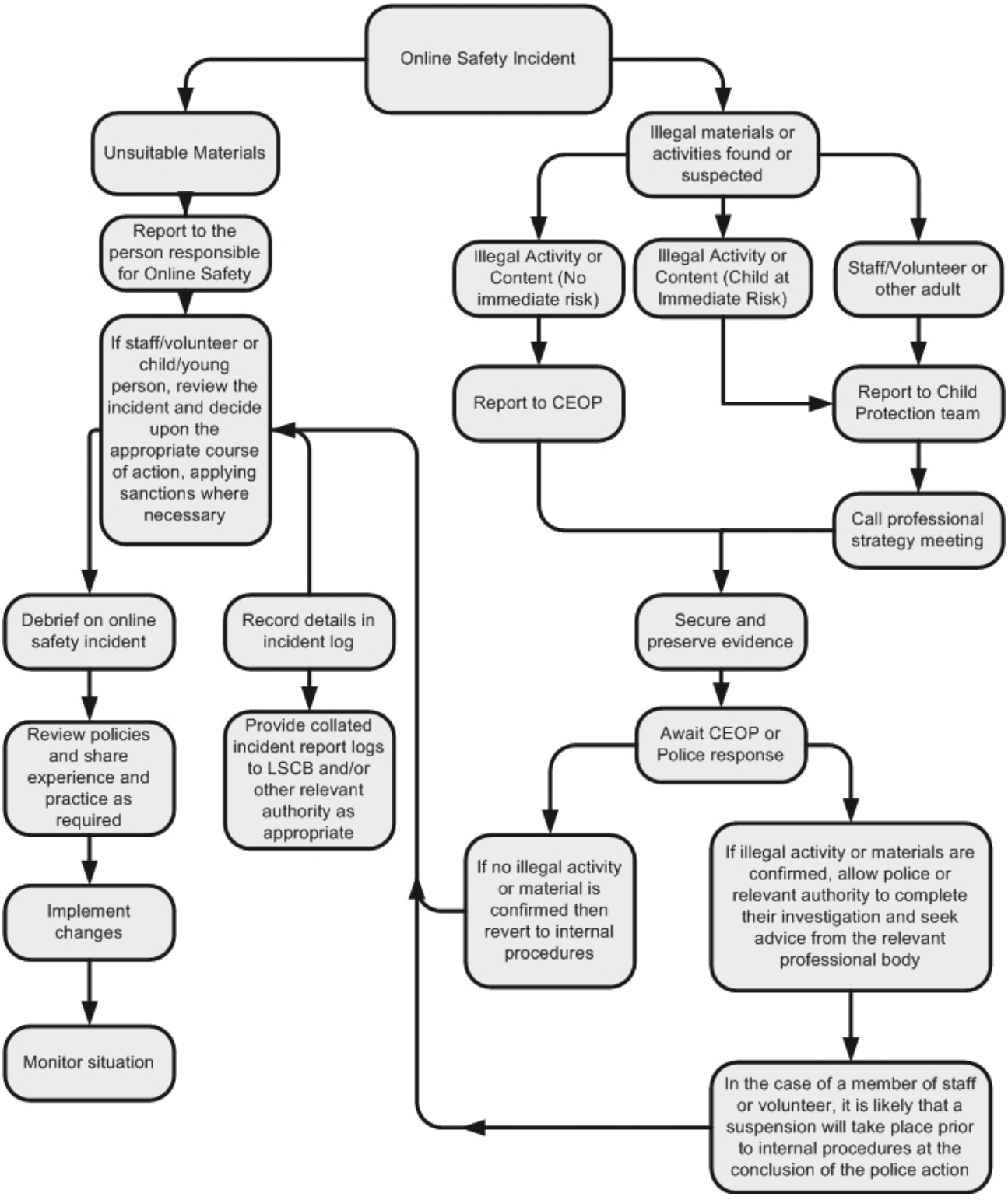
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the

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:

A.2.7 Reporting of e-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.

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

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 should be 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 Mobile Technology (tablets, phones etc)

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

- Personal IDs (often with associated personal media collections, eg music from iTunes) are not to be used on school owned devices.
- It is not permissible for children to have access to staff tablets unless very carefully supervised.
- All data is removed from tablets before it is allocated to a different member of staff.
- Individual teachers are responsible for ensuring that any data, apps, photographs etc stored on the iPad are appropriate and professional. This is particularly important when mirroring to interactive whiteboards / screens.
- Cloud storage (other than officially endorsed systems) is not used for sensitive data.

- 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

- Please see staff and governors confidentiality agreement, signed by all staff

A.3.1c – School Owned devices used by pupils

- iPads are managed locally using Apple Configurator on a school owned MacBook.
- 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, Google Apps for Education, Showbie etc…).
- We make use of cloud services in other carefully chosen apps
- 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:

- Pupils are not currently permitted to bring their personal hand held devices into

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 (eg by remote access).
- Users need to be aware that email communications will be monitored
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy)
- 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 communication.

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
- 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.

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

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

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

A.3.3 Use of digital images (still and video)

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. See also section 3.1 for guidance on type of device used to capture / store images.
- 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.

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.

- Personal information should not be posted on the school website and only official email addresses (ideally as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).

- Detailed calendars are not published on the school website.
- Photographs / video published on the website, or elsewhere, that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)
    - See also section A.3.3
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

A.3.4b – 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 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 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

Teachers frequently discuss issues relating to password security and how it relates to staying safe in and out of school

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 from *Enter the name of your internet service provider here* and we automatically receive the benefits of a managed filtering service, *enter the name here*, 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 schools IT provider in conjunction with 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.

All users have a responsibility to report immediately to class teachers / e-safety coordinator any infringements of the school's filtering systems 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 e-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 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.

Section C. Education

C.1.1 E-safety education

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

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

- A planned e-safety programme should be provided as part of Computing, PHSE and other lessons and should be regularly revisited – this will cover the use technology in school and outside school
- We use the Digital Literacy resources within the Herefordshire Computing Progression. This scheme draws on resources from a number of highly regarded sources.
- Learning opportunities for e-safety are built into the Herefordshire Primary Computing Progression where appropriate and are used by teachers to inform teaching plans.
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP (see Appendix 1) and encouraged to adopt safe and responsible use of 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 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 Herefordshire Computing Progression to deliver our computing curriculum. The digital literacy section of this signposts age appropriate resources from a good range of providers which forms the basis of our e-safety education in school.

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:

- The school constantly monitors staff training needs and a programme of e-safety training will be made available to staff.
- All new staff should ensure 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 information / training sessions and by reviewing guidance documents released by the DfE, local authority, the HSCB and others.
- The E-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 e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in IT, 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, national or local 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
- Referring parent to a range of online resources (saferinternet.org.uk, internetmatters.org …)

C.5 Wider school community understanding

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

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.