Shires Multi Academy Trust	With God we grow to live life in all its fullness	
E-Safety Policy **Policy Number: FPS/0012**	**Issued**: March 2022	**Issued by**: J Little - Headteacher

Feckenham CE Primary School

E-SAFETY POLICY

Date Policy Reviewed:	March 2022	
Date Approved By Governing Body:	24.03.22	
Signed Headteacher:		Jeannette Little
Signed Chair of Governors:		Julie Grieve
Review Date	March 2023	

Safeguarding Children in a Digital World

Introduction

This Policy has been developed to ensure that all adults in Feckenham CE Primary School are working together to safeguard and promote the welfare of children and young people.

E-Safety is a safeguarding issue, alongside an ICT issue and all members of the school community have a duty to be aware of E-Safety at all times, to know the required procedures and to act on them.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit of using ICT, whilst minimising associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its "Safeguarding Children in a Digital World" suggested:

> *"That schools support parents/carer in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school/academy links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."*

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 School and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

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 and young people, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that children and young people learn and are taught. At home, technology is changing the way children and young people 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
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- 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 or addictive use which may impact on social and emotional development and learning.
- The potential to be drawn into terrorism through radicalisation via social media

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

Our e-safeguarding policy has been written from a template provided by Worcestershire County Council which has itself been derived from that provided by the South West Grid for Learning.

The main areas of risk for our school community are:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with racist language), substance abuse
- Lifestyle website, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Sexting
- Cyber-bullying
- Identity theft (including 'frape' (hacking Facebook profiles)), and sharing of passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and Well-Being (amount of time spent online including social media and gaming)
- Sexting (including sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership –such as music and film)

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 school council

The whole school council discusses issues relating to e-safety and when appropriate the staff representatives ask our school e-safety coordinator to lead assemblies on issues. Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as the Worcestershire Safeguarding Children Board – Family Front Door.

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:

- 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 ICT technical staff
- liaises with the Local Authority and relevant agencies
- attends relevant meetings and committees of Governing Body
- reports to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively
- Regularly updated in E-Safety issues and legislation, and is aware of the potential for serious child protection issues to arise from: • Sharing of personal data • Access to illegal / inappropriate materials • Inappropriate online contact with adults / strangers • Potential or actual incidents of grooming • Cyber-bullying and use of social media

A.1.3 Responsibilities: governors

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:

- Ensuring that the school follows all current E-Safety advice to keep the children and staff safe
- Supporting the school in encouraging parents and the wider community to become engaged in E-Safety activities
- meetings with the E-Safety Co-ordinator with an agenda based on:
    - *monitoring of e-safety incident logs*
    - *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 all 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 will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff. (See flow chart on dealing with e-safety incidents (included in section 2.6 below) and other relevant Local Authority / HR disciplinary procedures) receives reports of e-safety incidents and creates a log of incidents to inform future e-safety development.

- reviews weekly the output from monitoring software and initiates action where necessary
- meets with e-safety governor to discuss current issues and review incident logs

A.1.5 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of pupils and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school**.
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices, including the school's approach to the Prevent Agenda.
- they are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified
- they have read, understood and signed the school's Acceptable Use Agreement for staff (see Appendix 1)
- they report any suspected misuse or problem to the E-Safety Co-ordinator an safe guarding lead
- they undertake any digital communications with pupils (email / seesaw/zoom) in a fully professional manner and only using official systems (see A.3.5)
- they embed e-safety issues in the curriculum and other activities, also acknowledging the planned e-safety programme (see section C)
- To model safe, responsible and professional behaviours in their own use of technology

A.1.6 Responsibilities: ICT technician

Currently, as a school we 'buy in' technician support fortnightly. The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure and data are secure and not open to misuse or malicious attack after working on site
- the school meets the e-safety technical requirements outlined in section B.2.2 of this policy
- users may only access the school's networks through a properly enforced password
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.
- appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- reporting any E-Safety related issues that arises, to the E-Safety coordinator.
- that users may only access the school's networks through an authorised and properly enforced password protection, in which passwords are regularly changed
- to ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date
- that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- The school's policy on web filtering is applied and updated on a regular basis
- To ensure that all data held on pupils on the school office machines have appropriate access controls in place

A.1.7 Responsibilities: Pupils

- Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (N.B. in EYFS it would be expected that parents / carers would sign on behalf of the pupils)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To understand the importance of reporting abuse, misuse or access to inappropriate materials

- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home

A.1.8 Responsibilities: Parents

- To support the school in promoting E-Safety and endorse the Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children
- To access the school website / online student / pupil records in accordance with the relevant school Acceptable Use Agreement.
- To consult with the school if they have any concerns about their children's use of technology

A.2.1 Policy development, monitoring and review

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

- *E-Safety Coordinator – Mrs. O'Donnell*
- *Safeguarding officer – Mrs. Little*
- *Head teacher – Mrs. Little*
- *Teachers*
- *Support Staff*
- *Governors (especially the e-safety governor)*
- *Parents and Carers*
- *Pupils – Whole School Council*

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

- *Staff meetings (Zoom staff meeting due to Covid 19)*
- *Governor's meeting / subcommittee meeting*
- *School website / newsletters*

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:	*Mrs. O'Donnell and Mrs Little*
Monitoring of this policy will take place at regular intervals:	*12 monthly or sooner if needed*
The governing body will receive regular reports on the implementation of the e-safety policy group (which will include anonymous details of e-safety incidents) as part of a standing agenda item with reference to safeguarding:	Governors meeting termly
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*February 2023*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Worcestershire Safeguarding Children Board via Family Front Door* *Local Authority Designated Officer* *Worcestershire Senior Adviser for Safeguarding Children in Education* *West Mercia Police*

A.2.2 Policy Scope

This policy applies to **all members of Feckenham CE Primary community** (including teaching staff, wider workforce, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, **both in and out of the establishment**.

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 site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, radicalisation or other e-safety incidents covered by this policy, which may take place out of the school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as 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 Agreements

All members of the school community including technicians, whether directly employed or from external technical support teams, are responsible for using the school/academy ICT systems in accordance with the appropriate Acceptable Use Agreement (AUA), which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils
- Staff (and volunteers)

- Parents / carers
- Community users of the school/academy's ICT system
- Technical support personnel

Acceptable Use Agreements are introduced at parents' induction meetings and signed by all pupils as they enter school (with parents possibly signing on behalf of children below Year 2).

Pupils re-sign on entering a new Key Stage.

Acceptable use agreements discussed with all pupils at the start of each year

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

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school's ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school's ICT system.

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

A.2.4 Self Evaluation

Evaluation of e-safety is an ongoing process and links to other self-evaluation tools used in school in particular 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 and **Computing curriculum- ICT Progression**	How ICT is used, managed, resourced and supported in our school. Key documents and associated resources directly relating to learning covering the Computing Curriculum
E-Safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The e-safety policy constitutes a part of the ICT policy.

Other policies relating to e-safety

Anti-bullying	How your school strives to eliminate bullying – link to cyber bullying
PSHE and RSE	E-Safety has links to staying safe
Safeguarding	Safeguarding pupils electronically is an important aspect of E-Safety. ***The e-safety policy forms a part of the school's safeguarding policy***
Behaviour	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 an education 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, transfer data, 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 including radicalisation as per the Prevent Agenda (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 equipment or infrastructure provided by the school:

- *Using school systems to undertake transactions pertaining to a private business*
- *Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband and / or the school*
- *Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions*
- *Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)*
- *Creating or propagating computer viruses or other harmful files*
- *Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)*
- *On-line gambling and non-educational gaming*
- *On-line shopping / commerce unless directly related to school/academy business*
- *Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)*

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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 indicated on the following pages:

	Refer to:					Inform:	Action:		
Pupil sanctions	Class teacher	E-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator for action re filtering / security etc	Parents / carers	Remove of network / internet access rights	Warning	Further sanctions e.g. 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/academy network by sharing username and passwords	✓	✓	✓		✓		✓	✓	
Attempting to access the school/academy network, using another pupil's account	✓				✓		✓		
Attempting to access or accessing the school/academy 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/academy into disrepute or breach the integrity of the ethos of the school/academy	✓		✓					✓	
Using proxy sites or other means to subvert the school/academy'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	✓		✓		✓		✓		

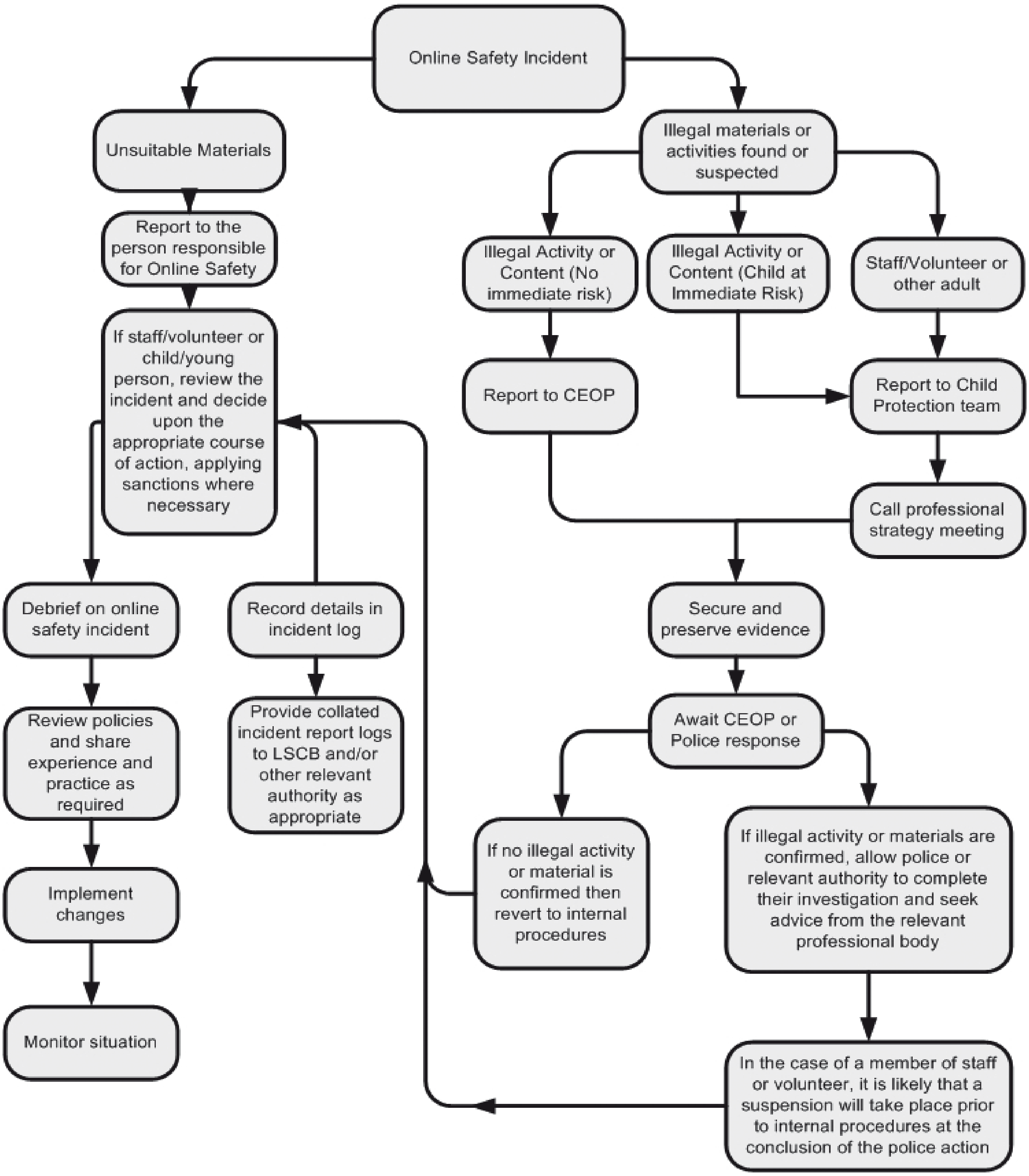
	Refer to:					Action:		
Staff sanctions	E-Safety Co-olrdinator	Head teacher	Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier 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/academy network by sharing username and passwords or attempting to access or accessing the school/academy network, using another person's account	✓	✓			✓	✓	✓	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓	✓		✓	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓		✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓				✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓				✓	✓	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓			✓	✓	✓	
Actions which could compromise the staff member's professional standing	✓	✓						
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy	✓	✓				✓		
Using proxy sites or other means to subvert the school/academy'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, 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
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
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
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.3.1 Use of hand held technology (personal phones and other 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.*
  - ✓ *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 outside teaching time.*
  - ✓ *The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.*
  - ✓ *Mobile phones brought into school are entirely at the staff member, parent or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school*
  - ✓ *The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones*

- *Pupils are not currently permitted to bring their personal hand held devices into school.*
- *A number of such devices are available in school (e.g. iPad, I-pod Touch) and are used by pupils 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 s. permission	Not allowed
Mobile phones may be brought into the school/academy	✓						✓	
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time		✓						✓
Taking photos on personal phones or other camera devices				✓				✓
Use of hand held devices e.g. PDAs, gaming consoles	✓						✓	

A.3.2 Use of communication technologies

A.3.2a – Email

Access to email is provided for all schools using Worcestershire schools' broadband via their Global IDs.

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

Feckenham CE Primary School will ensure:

- Staff and pupils should use only the school email services to communicate with others regarding school business 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 teacher*
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy)
- *Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (if they are not blocked by filtering)*
- Users must immediately report to their teacher / e-safety coordinator – in accordance with this policy (see sections A.2.6 and A.2.7) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such email.
- Members of staff to use _______ when sending emails with personal and sensitive information
- It does not publish personal email addresses of pupils or staff on the school website
- To contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law
- that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a broadband filter to help protect users and systems in the school, also including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, smoothwall monitoing monitors and protects our Internet access to the World Wide Web

Pupils:

• We use Worcestershire Global ID's for email addresses with pupils

* Pupils' Global ID's e-mail accounts are intentionally 'anonymised' for their protection

• Pupils are introduced to, and use email as part of their computing scheme of work in keystage 2

• Pupils are taught about the safety and 'netiquette' of using email both in school and at home i.e. they are taught:

> Not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer

> That an email is a form of publishing where the message should be clear, short and concise

> That any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper

> They must not reveal private details of themselves or others in email, such as address, telephone number, etc.

> To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe

> That they should think carefully before sending any attachments

> Embedding adverts is not allowed

> That they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature

> Not to respond to malicious or threatening messages

> Not to delete malicious of threatening emails, but to keep them as evidence of bullying

> Not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them

> That forwarding 'chain' email letters is not permitted

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

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

• Teachers are instructed not to run social media spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

• The school's preferred system for social networking will be maintained in adherence with the communications policy. We do not permit use of Facebook, Twitter or any other social network sites within lesson time

- School staff will ensure that in private use:
- • No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or MAT
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.

	Staff / adults				Pupils			
Use of social networking tools within school time	Allowed	Allowed at certain times	Allowed for	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.3.2c - Videoconferencing

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

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

Only web based conferencing products that are authorised by the school (and are not blocked by internet filtering) are permitted for classroom use.

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

Permission for pupils to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in the school (see section A.2.3 and Appendix 1). Only where permission is granted may pupils participate.

Roles and Responsibilities of the host

The person hosting the meeting will:

- Ensure there is a secure mechanism for all parties to have a virtual presence at the meeting
- Ensure there is a suitable, secure online meeting platform or telephone link.
- Share the Protocols prior to the meeting

Meeting Protocols if the school is the host:

- Ensure that all parties are included into communications regarding the organisation of the meeting
- Access arrangements should be shared in advance of the meeting by the host; these should include how to connect to the meeting and if software is needed to be downloaded to enable parties to join this should be circulated
- Ensure all contact details (email and phone) held are up to date, in case there is a need to contact prior to or as an alternate prior to the meeting.
- Any papers to be considered will be circulated in advance of the meeting and confirmation they will be shredded at the end of the meeting
- Where appropriate, all parties should have a trial call for the first virtual meeting to ensure that everyone is able to establish connection.
- Ensure that any technical difficulties can be overcome as quickly as possible.
- All parties should know the hosts' contact number should they have technical difficulties in joining the meeting so that they can make contact to ensure that there is no unnecessary delay.
- Connect to the meeting a few minutes prior to meeting start time to ensure that the meeting can run to time with minimal interruptions.
- The host should ensure at the start of the virtual meeting that introductions are made including name and role in meeting, where appropriate.
- Time delays can happen, so make sure everyone has the opportunity to participate and ask questions. All parties should be reminded of the School's IT acceptable use policy and data security policy at the beginning of all proceedings. Reminders are made about confidentiality and information being shared after the meeting
- Virtual meetings should not be electronically recorded by any persons attending the meeting. Parties will be reminded by the host at the start of the meeting that recording of the meeting will not be permitted except in exceptional circumstances (for example as a reasonable adjustment for a disabled participant at the hearing). Action under the Disciplinary Procedure may be taken if any covert recording is undertaken.
- Remind parties to consider the surroundings in which they will be taking the call. Ensure that your location has good Wifi, an electrical power source, is reasonably quiet and private to ensure that the content of the call is only heard by the intended recipients. If video, to be aware of what will be on camera. If using a handheld device, they should consider how long they will be on the call for and consider using a handsfree device for their own comfort.
- If they are in a location with lots of background noise, mute their microphone when not speaking – this improves call quality for everyone.
- State their name when they are talking on the call, this is especially important if not on video conferencing.
- The host needs to try to give time for all parties to have their input into the meeting, allowing for everyone's input to be included.

- Parties should respect other attendees and allow others to finish before speaking. The agenda /order of proceedings for specific meetings will be made advance.
- The host will ensure that minutes of the meeting are taken and that there is a note that the meeting was held through teleconference/video link in the minutes.
- The host to ensure that all parties are aware of any actions points or next steps before closure of meeting.

Meeting Protocols if the school is not the host:

- Share their protocols for the meeting. If there are none then ask the host to:
  - ➢ Confirm with all parties that the virtual or telephone meeting will not be electronically recorded by any parties attending the meeting
  - ➢ Remind all parties about confidentiality and information being shared after the meeting and any paper documentation is shredded
  - ➢ Ask parties to confirm the surroundings in which they will be taking the call content and that it is only heard by the intended recipients. If video is also being used, to be aware of what will be on camera
  - ➢ Ask all parties to identify themselves by name at the start of the meeting and when speaking during the meeting
  - ➢ Ask for all parties to be visible throughout the meeting where possible for identification

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 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.

- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share/publish their photograph (e.g. some looked after children)

- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section (A.3.4) for guidance on publication of photographs

A.3.4 Use of web-based publication tools

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

Our school uses the public facing website www.feckenhamceprimary.co.uk and the twitter page – Feckenham School, only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of pupils. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website or twitter and only official email addresses will be used to identify members of staff (never pupils).

- *Only pupil's first names will be used on the website and twitter, and only then when necessary.*

- Detailed calendars will not be published on the school website or twitter.

- Photographs published on the website, twitter 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)

A.3.4b – Learning Platform - SEESAW

Teachers monitor the use of the learning platform (Seesaw) by pupils and parents/carers regularly during all supervised sessions, but with particular regard to messaging and communication. Currently messaging between pupils is not possible and private messaging school staff is switched off. Staff can send whole class messages on the learning platform and personal responses to children's work on the pupil's journal page. Teachers have to approve all work and comments from pupils and parents/carers before it is uploaded to the journal.

Parents/Carers must sign a permission GDPR data form before a child's account is created.

Parents/Carers must give signed permission before their child's image can be uploaded to Seesaw. A separate letter will be issued once an account has been created. Where parents/carers do not give permission, no images or videos of their child will be used on seesaw.

No surnames will be used on a seesaw account. Where there are children with the same name in the same year group, surname initials will be used only to help staff identify whose work is whose.

Staff use is monitored by the super-user/administrator.

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 access to the learning platform.

When staff, pupils, etc. leave the school their account or rights to specific areas will be disabled (or transferred to their new establishment if possible / appropriate).

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the learning platform may be suspended for the user.

d) The user will need to discuss the issues with a member of SLT before reinstatement.

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

A visitor may be invited onto the learning platform by the administrator following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

A.3.5 Professional standards for staff communication

In all aspects of their work in our establishment, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA effective from September 2012: 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, learning platform, 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

* Feckenham CE Primary School makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it

• All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private

• We require staff to use STRONG passwords for access into our Arbor system

The school e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school. (See section C of this policy)

B.2.1 Filtering

B.2.1a - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can, 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 an educational broadband services provided by Entrustl, we automatically receive the benefits of a managed filtering secure broadband service, with some flexibility for changes at local level.

Feckenham CE Primary School uses Smoothwall Monitor to ensure any online incidents are detected on our network and school equipment. Smoothwall is installed on all pcs and ipads.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by our IT Technical support - Lourdes, (with ultimate responsibility resting with the **head teacher and governors**). They manage filtering in line with this policy 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 Worcestershire, or other, school filtering service must:

- be logged in change-control logs by the person making the change
- *be reported to a second responsible person (the head teacher / e-safety coordinator / e-safety governor) within the time frame stated in section A.1.3 of this policy*

  Or
- *be reported to, and authorised by, a second responsible person prior to changes being made*

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

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 Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

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

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, 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.

THEN

- *If agreement is reached, the e-safety coordinator makes a request to Lourdes IT Team*
- *The team will endeavour to unblock the site within a reasonable time. This process can take a number of hours so teaching staff are required to check websites well in advance of teaching sessions.*

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.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the network and on school equipment using Smoothwall Monitoring.

Monitoring takes place as follows:

- At least 2 identified members of staff (Mrs Little and Mrs Lightfoot and Mrs O'Donnell) review the monitoring console captures in turn, weekly.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

B.2.1f - Audit / reporting

Filter change-control logs and incident logs are made available to:

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

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

B.2.2 Technical security

This is dealt with in detail **by Consero IT Technical Team**

To ensure the network is used safely, Feckenham CE Primary School:

- Ensures staff read and sign that they have understood the school's E-Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes
- We provide pupils with an individual network log-in username in Keystage 2

- We use the Worcestershire Global ID system for username and passwords
- Staff use Egress (a secure data security software) to send emails with personal and sensitive information.
- Make it clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 10 minutes and have to re-enter their username and password to re-enter the network.]
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also switch off all computers at half past 5 to save energy
- Has set-up the network so that users cannot download executable files / programmes
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes
- Any user bringing in their own device is responsible for ensuring their device has upto-date security software
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use".
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed e.g. projector filters cleaned by clearner in charge / TA, equipment installed and checked by approved Suppliers / LA electrical engineers
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements
- Uses the DfE secure s2s website for all CTF files sent to other schools
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Our wireless network has been secured to industry standard Enterprise security level/appropriate standards suitable for educational use
- All computer equipment is installed professionally and meets health and safety standards
- Projectors are maintained so that the quality of presentation remains high
- Reviews the school ICT systems regularly with regard to health and safety and security

B.2.3 Personal data security (and transfer)

This is dealt with in detail in **Lourdes School's System and Data Security advice**. Please see that document referred to in the introduction for more information.

Teachers 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 constant help and support to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping them to learn how 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 progressive e-safety programme is taught as part of Computing, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and beyond school. At Feckenham CE Primary, we follow the education programme from 'ThinkUKnow' for 4-7 and 8-10. We use 'Switched on Computing' and 'PSHE Association'. This covers a range of skills and behaviours appropriate to their age and experience, including:
- At the end of Year 6, pupils should know:
    - ➢ That people sometimes behave differently online, including by pretending to be someone they are not.
    - ➢ That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
    - ➢ The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, how to report them.
    - ➢ How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
    - ➢ How information and data is shared and used online.
    - ➢ That for most people the internet is an integral part of life and has many benefits.
    - ➢ About the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content on their own and others' mental and physical wellbeing.
    - ➢ How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
    - ➢ Why social media, some computer games and online gaming, for example, are age restricted.
    - ➢ That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
    - ➢ How to be a discerning consumer of information online including understanding that information, including that from search engines is ranked, selected and targeted.
    - ➢ Where and how to report concerns and get support with issues online Teaching

    Online Safety in School (2019) and RSE (2020)

- Key e-safety messages will be reinforced through further input via assemblies as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the pupil Acceptable Use Agreement (see Appendix 1) and encouraged to adopt safe and responsible use of ICT both within and outside the school.
- *In lessons where internet use is pre-planned, it is best practice that younger pupils should be guided to sites checked as suitable for their use.* Processes should be in place, and known to pupils, for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging pupils to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

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
  - ✓ Referring to other (including non-digital) sources
- Pupils will 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 part for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/. These are mediated by a CEOP trained teacher.*

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

It is our general policy to encourage pupils to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Pupils often use technology out of the school in ways that we do not in education and members of staff are always keen to hear of their 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 – including non-teaching 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.
- *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 Agreements, which are signed as part of their induction
- The E-safety Co-ordinator (or another member of staff such as the Safeguarding Officer) will be CEOP trained.
- *The E-Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, OFSTED, the WSCB 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 ongoing basis.*
- *External support for training, including input to parents, is sought from appropriately qualified persons when required.*

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 School Improvement 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 their 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*

- *Curriculum evenings*

C.5 Wider community understanding

Messages to the public around e-safety should also be targeted towards grandparents and other adults engaging with pupils. Everyone has a role to play in empowering young people to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep them safe in the non-digital world.

Community Users who access school ICT systems / website as part of extended school provision will be expected to sign a Community User Acceptable Use Agreement (see Appendix 1) before being provided with access to school systems.

C.6 Handling Complaints

The school will take all reasonable precautions to ensure children are safe online in school. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Staff and pupils are given information about infringements in use and possible sanctions as detailed above in A.2.6

Appendix 1 – Acceptable Use Agreement templates

Acceptable Use Agreement – pupil (KS1)

This is how we stay safe when we use computers:

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

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

My name:	
Signed (child):	
OR Parent's/Carer's signature:	
Date:	

Acceptable Use Agreement – pupil (KS2)

I understand that while I am a member of Feckenham C.E. Primary School, I must use technology in a responsible way.

For my own personal safety:

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

For the safety of others:

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

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal device if I have permission and use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on devices belonging to the school without permission.
- I will only use social networking, gaming and chat through the sites the school allows

KS2 Pupil Acceptable Use Agreement Form

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

Name:	
Signed:	
Date:	

Acceptable Use Agreement – staff & volunteer

Background

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

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

For my professional and personal safety:

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

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

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

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

- I will only use my personal mobile ICT devices as agreed in the e-safety policy (see section A.3.1) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems except in an emergency (A.3.2).
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or radical material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school/academy policies.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy. **I understand that where personal data is transferred outside the secure school network, it must be encrypted.**
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

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

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

Staff / volunteer Name:	
Signed:	
Date:	

Acceptable Use Agreement and permission forms – parent / carer

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

This Acceptable Use Agreement is intended to ensure that:

- young people will be responsible users and stay safe while using ICT (especially the internet).
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of their work.

Child’s name	
Parent’s name and signature	
Date:	

Permission for my child to use the internet and electronic communication

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

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

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

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

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

Parent’s signature:	
Date:	

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

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

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

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

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

I agree that if I take digital or video images at school events which include images of children, I will abide by these guidelines in my use of these images. I agree that I will not post such images of children, other than my own, on social networking sites.

Parent's signature:	
Date:	

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

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the website or blogs.

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

Parent's signature:	
Date:	

Permission to for my child to participate in video-conferencing

Videoconferencing technology is used by the school in a range of ways to enhance learning – for example, by linking to an external "expert", or to an overseas educational partner. Video conferencing only takes place under teacher-supervision. Independent pupil use of video-conferencing is not allowed.

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

Parent's signature:	
Date:	

The school's e-safety Policy, which contains this Acceptable Use Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Acceptable Use Agreement – community user

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

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

I will be responsible in my communications and actions when using the school/academy ICT systems:

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

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

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

I have read and understand the above and agree to use the school ICT systems (both in and out of the school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school/academy as a direct result of my actions.

Community user Name:	
Signed:	
Date:	

Appendix 2 - Guidance for Reviewing Internet Sites

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. *This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software.* 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 abuse then the monitoring should be halted and referred to the Police immediately. 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.

A sample document for recording the review of and action arriving from the review of potentially harmful websites can be found on the next page

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

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 are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

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

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- 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**
- The content of the website is current.

C. 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?

D. ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Appendix 4 - Supporting resources and links

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

General

South West Grid for Learning "SWGfL Safe" - http://www.swgfl.org.uk/Staying-Safe

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

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

ChildNet http://www.childnet.com/

InSafe http://www.saferinternet.org/

Byron Reviews ("Safer Children in a Digital World") - https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

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

London Grid for Learning - http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety

Northern Grid - http://www.digitallyconfident.org

National Education Network - http://www.nen.gov.uk/e-safety/

WMNet – http://www.wmnet.org.uk

EU kids Online - http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/Home.aspx

Cyber Bullying

Teachernet "Safe to Learn – embedding anti-bullying work in schools" (Archived resources)

http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/academy/behaviour/tacklingbullying/cyberbullying/

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

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

CyberMentors: young people helping and supporting each other online - http://www.cybermentors.org.uk/

Prevent Duty - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Social networking

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

Get Safe On-line - https://www.getsafeonline.org/social-networking

Connect Safely - Smart socialising: http://www.connectsafely.org/

Mobile technologies

"How mobile phones help learning in secondary schools":

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf

"Guidelines on misuse of camera and video phones in school/academies"
http://www.dundeecity.gov.uk/dundeecity/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

Digital Parenting - http://www.vodaphone.com/parents

http://www.digitalparenting.ie/

https://www.commonsensemedia.org/

Links to other resource providers

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school/academy staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website: http://www.swgfl.org.uk/staying-safe

BBC Webwise: http://www.bbc.co.uk/webwise/

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

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

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

Internet Watch Foundation: http://www.iwf.org.uk

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

Appendix 5 - Glossary of terms

AUA	Acceptable Use Agreement – 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 archived and still relevant)
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
ICT	Information and Communications Technology
ICT Mark	Quality standard for school/academys provided by NAACE for DfE
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 Regional Broadband Consortia
KS1; KS2	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
Learning Platform	An online system designed to support teaching and learning in an educational setting
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 school/academys 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 school/academies 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 – a web address
WMNet	The Regional Broadband Consortium of West Midland Local Authorities – provides support for all school/academys in the region and connects them all to the National Education Network (Internet)
WSCB	Worcestershire Safeguarding Children Board (the local safeguarding board)

Appendix 6 Template Reporting Log

Reporting Log

Group ………………………………………………………….

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix 7 Guidance to support the safe and appropriate use of images in schools and settings

Based on:

Safeguarding Children and Safer Recruitment in Education – *Consultation version 2010*

Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings – *DCSF March 2009*

Data Protection Good Practice Note: Taking Photographs in School – *Information Commissioner's Office 26th October 2007*

Please ensure that all staff are given copies of this guidance and made aware of school policy

Introduction

There are many occasions when staff and parents will want to take photographs of children. Such occasions include everything from observation, evidence, assessment and curricular purposes in the classroom to award ceremonies, performances, trips and sporting events as part of the extended activities programme. The intention of this policy is to set out clear guidelines which will balance the use of photography as a source of pleasure and pride with the need to safeguard children and protect the rights of the individual.

The photography policy sets out to ensure that:

- Photographs are only used for the purpose intended
- Settings use of photographs is facilitated
- Personal family photography is allowed where possible
- Individual rights are respected and child protection issues considered
- Parents/carers and children are given the right to opt out.

Definitions

The term 'images' refers to photographic prints or slides, digital images, videos or moving images. Images may be distributed via print, DVDs, the internet or other technologies.

The term ' settings' refers to Early Years Settings, Maintained Schools, Independent Schools, Free Schools, Academies, Short Stay Schools, Colleges of Further Education, out of school provision, childminders and Children's Centres.

Safeguarding Children

The welfare and protection of our children is paramount and consideration should always be given to whether the use of photography will place our children at risk. Images may be used to harm children, for example as a preliminary to 'grooming' or by displaying them inappropriately on the internet, particularly social networking sites.

For this reason consent is always sought when photographing children and additional consideration given to photographing vulnerable children, particularly Looked After Children or those in domestic abuse situations. Consent must be sought from those with parental responsibility (this may include the Local Authority in the case of Looked After Children).

Data Protection

The Information Commissioner’s Office (ICO) maintains a public register which includes the name and address of 'data controllers' and details about the types of personal information they process. 'Notification' is the process by which each data controller’s details are added to the register. All settings need to ensure they are registered with the Information Commissioner's Office every year. Failure to notify the ICO is a criminal offence. Notification is necessary if settings are processing personal information. This includes taking photographs of the children using a digital camera. Personal data (including photos) held by settings must be included in the setting's notification. Further information on data protection as well as details on how to notify can be found at:http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx

Please note that although notification is mandatory in most cases the data protection guidance within this document is 'recommended guidance' and settings must take individual responsibility for their own data protection issues in accordance with the new GDPR 2018

Parental Consent

On admission of a child to a setting, parents/carers will be asked to complete a consent form indicating their agreement or objection regarding the use of images of their child. Consent should be discussed with the child, once they are old enough to understand, and the child also asked to sign the consent form. Parents/children should be asked to complete the separate WCC consent form for images that have been taken for the purpose of LA publicity.

A list of children for whom consent has been refused will be maintained by the setting and every effort will be made by staff not to include these children in photographs or video footage. The list will be updated on a regular basis[1].

The parent/carer should be asked to confirm, in writing, that they will inform the setting if they no longer wish images of their child to be used for any reason. They need to be made aware that once images are in circulation or have been published, it may be impossible to remove them, although every effort will be made to ensure they are not used in future publications.

Setting Photography

Photographic and/or video images taken by staff may be used for curricular and/or extra-curricular activities, displays, on the setting website, in the setting prospectus or newsletter, as evidence of the child's development or as part of publicity in the media. Staff will ensure that:

- They are clear about the purpose of the activity and what will happen to the images when the activity is concluded.
- They always use setting equipment for taking images.
- They never record images using their personal camera, mobile phone or video equipment or for their own personal use.
- They will never photograph children in a state of undress, for example whilst changing for PE or a performance.
- They will report any concerns about inappropriate or intrusive photographs found to the Senior Designated Person following the setting's safeguarding procedures
- They have parental permission to take; store and/or display the images.
- Childminding settings should pay particular attention to the safe storage of digital imagery if using their personal equipment to record and store images

Storage of Images

Photographs retained in a setting will not be used other than for their original purpose, unless permission is obtained from the subject.

Images should always be stored securely and password protected.

Photographs should be destroyed or deleted from databases once they are no longer required for the purpose for which they were taken. Photographs taken for publicity and promotional purposes should be retained for a maximum of two years. Photographs contributing to the history of the setting, its children, activities or the community, may be retained indefinitely.

For schools, further information on storage and security can be found in the LA guidance *Schools System and Data Security.*

Parental Photography

In many cases, photographs taken at setting events form an important part of family albums. Everything possible will be done to ensure that this tradition continues. Parents are welcome to take photographs of their own children at award ceremonies, setting concerts/shows and sporting events, with the permission of the Headteacher/Senior Manager. However, care must be taken not to interfere with the smooth running of the event, breach commercial copyright laws or compromise health and safety. Parents/carers will ensure that:

[1] The LA recommends on admission to a setting with at least annual updates

- They will respect the setting's decision to prohibit photography of certain children or a particular event.
- Any images taken are for personal use only.
- Images including children **other than their own, must not be sold or put on the internet**; if they are, Data Protection legislation may be contravened and they will be asked to remove them.
- They will not use any images of children so as to cause offence or harm.

The Use of Cameras and Video Recordings by Children

From time to time, children may be given the opportunity to use setting equipment to take photographs and/or video footage as part of a curricular or extra-curricular activity.

Children should not use personal equipment in the setting for the purpose of taking photographs or video footage, unless being used as a learning resource in line with the setting's Acceptable Use policy. This includes the use of personal Smartphones. The only exception to this is on a setting trip or visit where children may be allowed to take photographs for their own personal use.

It should be made clear that these images should be taken responsibly and not used to upset any other child

The use of images to bully or intimidate, including publishing photographs without permission on the internet, will be dealt with in line with the setting's behaviour and anti-bullying policies and may be viewed as a criminal offence.

Display of photographs

It is perfectly acceptable to display photographs of children in the setting environment with their names attached for the purpose of celebrating progress and achievement or assessment purposes.

However, all settings must give consideration to displays when rooms are available for other purposes.

Publicity

Press

On occasions, the media are asked to cover setting events or to highlight children's successes. This is an important part of celebrating achievement and informing the public of educational initiatives. The media operate under their own Code of Practice. Parents will be informed by the setting in advance if their children are likely to appear in the press. Local newspaper titles may share their images with other titles within the same syndicate. Any child whose parents have withheld permission, will not be photographed by the media.

Setting Publicity

Photographs of children's activities and achievements may be published in the setting newsletter or prospectus and posted on the setting website. Names of individual children will not be attached to photographs and no contact details will be published. Where photographic permission has been withheld, photographs will not be published.

Setting Photographer

Class and individual or group photographs are often an annual event. Parents will be notified in advance of the photographer's visit and will be sent copies of photographs and given the option to purchase them. Copyright on all such photographs is retained by the photographer.

Links

This guidance should link specifically to the setting's Data Security Policy, E-safety Policy, Acceptable Use Policy, Password Policy, Staff Laptop Policy, Safeguarding Children Policy and to the LA guidance 'Schools System and Data Security'.

Further Guidance

Further related guidance can be found in the Becta series of documents entitled *Good practice in information handling in schools*. They are:

1 Keeping data secure, safe and legal
2 Impact levels and labelling
3 Audit logging and incident handling
4 Data encryption
5 Secure remote access
and also in *AUPs in context: Establishing safe and responsible online behaviours*
These documents can be found on Edulink (www.edulink.networcs.net) and on the Department for Education website (www.education.gov.uk

Consent Form for use of Images (photographs, videos, DVDs and digital images)

Photographs and/or video recordings of children may be taken whilst they attend the Feckenham C Primary School to celebrate their achievements and successes and as evidence of their progress and development. Still or moving images may be published in our printed publications (e.g. prospectus, newsletters) and/or on our external websites. They may also be used to promote the good practice of the setting to other teachers, e.g. at training events organised by the Local Authority or national education/government institutions. Children's names will never be published alongside their photograph externally to the education setting. Names may be used internally, for example – on a display.

Electronic images, whether photographs or videos, will be stored securely on the setting's network which is accessible only by authorised users.

Before using any photographs/videos of your child we need your permission. **Please answer the questions below, then sign and date the form where indicated and return it.**

Please circle

1. May we use your child's photograph in printed publications? **Yes / No**

2. May we use your child's photograph on our internet websites? **Yes/No**

3. May we allow your child's photograph (e.g. as part of a team or record of an event) to be used for publication in a newspaper? **Yes / No**
   (Please note that the use of photographs in newspapers is subject to strict guidelines)

4. May we use any photograph or video of your child internally as part of regular activities and work of the setting? **Yes / No**

5. May we use any photographs or video containing your child to share good practice with staff from other settings? **Yes / No**

6. May we use images of your child on an external web site or for publicity or campaigns by national Government agencies? **Yes/No**

This form is valid from the date of signing until your child leaves Feckenham CE Primary School. Photographs and videos may be securely archived after your child has left the setting. Photographs and videos used for publicity purposes may continue to remain in circulation after your child has left the setting. You may withdraw your consent, in writing, at any time **but it may not be possible to remove images that are already in circulation or have already been published** although every effort will be made to do so.

We recognise that parents, carers and family members will wish to record events such as plays, sports days etc. to celebrate their child's achievements. The school is happy to allow this, at the discretion of the Headteacher, on the understanding that such images/recordings are used for purely personal family use. **Images containing children other than their own should not be put on the internet for any reason, without first seeking permission from the other child's parents/carers.**

A full copy of the setting's policy on the safe use of children's photographs may be obtained upon request.

Name of Child: ……………………………………………… Date of birth: ………………………………

Signed: ………………………………………………… Date: ………………………

(if appropriate)

Name of person with Parental Responsibility: …………………………………………………

Signed: …………………………………………………. Date: ……………………

Data Protection

Feckenham CE Primary School takes your privacy seriously and we have taken steps to protect it. Any personal data you give to us, including photographic images, will be processed strictly in accordance with the new GDPR Act and will be used for the purposes that you have consented to. We will not share your details with third parties without your consent, except where we are legally compelled or obligated to do so. Please note that where you consent to images appearing on the internet, they can be viewed worldwide including countries where UK data protection law does not apply.

Appendix 8 Social Networking Teacher Agreement

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.

- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.

- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.

- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.

- Do not accept pupils (even those that have recently left the school)

- Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.

- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.

- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause friction in your school and make your working environment uncomfortable.

- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.

- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform Mrs Little. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.

I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.
I understand that injudicious use of social networking may lead to disciplinary action.
I agree to take all possible precautions as outlined above.

Name		***Date***	

Appendix 9 Loaned Device User Agreement

Staff member: Date:

Device Make: Model : Serial Number :

The laptop/device detailed above is loaned to ____________________________for the duration of their employment at Feckenham CE Primary School subject to the following terms and the school Acceptable Use Agreement.

The iPad/mobile device remains the property of the School and must be returned at the end of the contracted period of employment with the School and, if required, during a planned or prolonged absence.

1. The laptop/device is for the **work related** use of the named member of staff to which it is issued.
2. Only software/apps installed at the time of issue or software/apps purchased by and licensed to Feckenham CE Primary School may be installed on the machine.
3. The laptop/device remains the property of the School throughout the loan period, however the member of staff to which it is issued **will** be required to take responsibility for its care and safe keeping.
4. If left unattended the laptop/device must be securely stored. It must **never** be left unattended even for a short period in a car, including in a locked boot.
5. Due regard must be given to the security of the computer if using other forms of transport.
6. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality, under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff. Staff should also be cautious when using the computer away from school particularly with files which may contain personal student data, including images.
7. The equipment must be docked in the school charging and syncing cabinet at least once per week to ensure updates and new software are distributed. Staff should record this action in the log provided with the syncing cabinet.
8. The laptop/device will be recalled from time to time for routine maintenance / upgrade and monitoring.

Prohibited Uses

Images of other people, including children, may only be made with the permission of the person, or parents of the child, in the photograph.

The laptop/device is a professional tool designed to enhance classroom practice. It is not for personal use, e.g. Facebook or other social networking sites or on-line shopping.

Lost, Damaged or Stolen laptop/device

If the laptop/device is lost, stolen or damaged, the ICT Co-ordinator or Head Teacher must be informed immediately and a charge may be levied depending on the circumstances.

I have read and agree to the terms and conditions in this agreement.
I undertake to take due care of the laptop or device and return it immediately upon request.

Signed: ____

Date: ____

This policy should be read in conjunction with the school E-Safety Policy and the Safeguarding Policy and Procedures (including Child Protection). All our practice and activities must be consistent and in line with the Safeguarding Policy and Procedures noted above. Any deviations from these policies and procedures should be brought to the attention of the Mrs Little so that the matter can be addressed.