E-Safety Policy

Name & address of the premises	**The Ferncumbe C of E VC Primary School** **The Green** **Hatton** **Warwick** **CV35 7EX**
Person Responsible for day-to-day management of the premises **e.g. Head Teacher, Centre Manager**	Miss Sally Morris, Executive Headteacher Mrs Tracey Webb, Head of School
Name of person producing plan (print name)	Miss Charlotte Forbes
Next Review at Meeting	Feb 2024 - Spring 1 Meeting
Folder found in	Policies – Curriculum

E-Safety Policy

Contents

E-Safety Policy

Scope of the Policy

This policy applies to all members of the Ferncumbe Primary School community (including staff, pupils, volunteers, parents/carers, visitors) who have access to and are users of the school computing systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. **This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school**. The 2011 Education Act increased these powers with regard to the searching for and of electronic decides and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour policies and will, where know, inform parents / carers of incidents of inappropriate e-safety behaviour that has taken place out of school.

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups with Ferncumbe Primary School.

Governors

Governors are responsible for the approval and review of the effectiveness of the E-Safety policy, as well as the appointment of an Online Safety Governor. The Child Protection/Online Safety Governor will:

- Monitor E-Safety incident logs
- Report to relevant Governors meetings

Headteacher

The Headteacher has a duty of care for ensuring the online safety of members of the school community, though the day to day responsibility for e-safety will be delegated to the Online Safety Coordinator.

- The Headteacher should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. *(See flow chart on dealing with E-Safety incidents*).
- The Headteacher is responsible for ensuring that the E-Safety coordinator and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This will be done through training opportunities and local consortium meetings where issues can be raised.

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.

- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place
- Provides training and advice for staff
- Leads a yearly E-Safety week within school
- Liaises with the Local Authority / relevant body
- Liaises with Launch
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety documents
- Meets regularly with the Online Safety Governor to discuss/review incident logs/issues

Technical Providers (Launch systems and Warwickshire)

Ferncumbe's technical provider, Launch Systems, along with Warwickshire providers, will ensure the following:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required E-Safety technical requirements and any Local Authority E-Safety guidance that may apply
- That users may only access the networks and devices through properly enforced password protection
- That filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That Ferncumbe School keeps up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update the E-Safety coordinator as relevant
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / E-Safety Co-ordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated

Teaching and Support staff

Are responsible for ensuring that:

- They have an up-to-date awareness of E-Safety matters and of the current school E-Safety policy and practises
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problems to the Headteacher / E-Safety Coordinator for investigation / action / sanction
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed)
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place or dealing with any unsuitable material that is found in internet searches.
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and avoid plagiarism / copyright regulations

E-Safety Policy

Designated Safeguarding Lead

Is trained in Online Safety and aware of potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

- Are responsible for using school digital technology in accordance with the Student Acceptable Use Policy
- Must understand the importance of reporting abuse, misuse or access to inappropriate materials
- have a good understanding of research skills; avoid plagiarism and uphold copyright regulations
- Will be expected to know and understand policies on the use of mobile devices and digital cameras
- Know and understand policy of taking/using images and on cyber-bullying
- Should adopt good E-Safety practise 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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. At Ferncumbe Primary School, we will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters and information about E-Safety campaigns.

Parents and carers will be encouraged to support the school in promoting good E-Safety practice and following guidelines on the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in the school (where this is allowed)

Policy Statements

Education and Pupils

Educating pupils in E-Safety is an essential part of our provisions as we need to ensure that children can take a responsible approach in their use of digital media.

E-Safety is reinforced throughout the curriculum and embedded as part of our Computing curriculum. We provide a broad, relevant and age-appropriate learning through the following ways:

- Following the Warwickshire LA Computing Scheme of Work, which embeds E-Safety in its learning
- A designated week on E-Safety being taught every year, providing children with age-appropriate information and guidance
- Helping Pupils to understand the need for the 'Student Acceptable Use Agreement' and encouraging them to adopt safe and responsible use **both within and outside school**
- Staff acting as good role models in their use of digital technologies
- In lessons where internet use is pre-planned, it is best practice that Pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where Pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, or even filtering this by using a child friendly search engine such as www.swiggle.org.uk

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education and Parents/Carers

Parents / Carers play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information about awareness to parents and carers through:

- Letters, newsletters, website
- Curriculum activities
- Parents evenings / sessions
- High profile events – e.g. Safer Internet Day, E-Safety week

Education and Training - Staff / Volunteers

Training will be offered as follows:

- All new staff should receive E-Safety training as part of their induction training, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements.
- Staff training during staff meetings
- The Online Safety Coordinator will receive regular updates through attendance of external training events
- This E-Safety policy and its updates will be presents to and discussed by staff in staff meetings / INSET days
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

E-Safety Policy

Training – Governors

- Governors should take part in online safety training / awareness sessions pertinent to their roles. This may be: Attendance at training provided by the Local Authority or participation in school training / information sessions for staff or parents.

Technical

The school will be responsible for ensuring that the school infrastructure / network is safe and secure and that policies and procedures are approved and implemented. This will be done in the following ways:

- Working with Launch and Warwickshire LA to ensure safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- Children in Years 1-6 will all be provided with a personal username and password. Users are responsible for the security of their username and password. The password fits the LA guidance, whilst also being suitable for the child's age group
- All teaching staff are provided with a username and password and supply teachers and support staff are offered limited access through the school's Supply login
- The administrator passwords for the school ICT system, used by the Network Manager, must also be available to the Headteacher and Online Safety Coordinator and kept in a secure place.
- The Headteacher and IT Technicians are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchases against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered. There is a process to request changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering (allowing for different groups of users – staff and pupils)
- School staff regularly monitor the activity of pupils and record any infringements.
- Systems are in place for users to report any actual / potential technical incident/security breach to the relevant person
- Appropriate security measures are in place, through WLA/Launch to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date virus software.
- Only encrypted memory sticks are allowed by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Most staff now use OneDrive, provided by WeLearn365 which meets regulations and is secure.

Use of Digital and Video Images

Digital imaging technologies have significant benefits to learning. Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- When possible, parents / carers will be given opportunities at the end of school events (such as assemblies and plays) to take digital images of their own child for personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, images containing other children should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images except for those on school feeds (such as through the school twitter page). Parents/Carers are warned/advised of this at the beginning or end of such events.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution, and publication of those images.
- If publishing photographs on the class twitter page, images should include multiple pupils and should not have any names written in conjunction with it
- Images should only be taken on school equipment; **the personal equipment of staff should not be used for such purposes.**
  must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Pupils' photos can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR 2016) – please see separate policy documents. Staff must ensure that they:

- Aware realise that they are personally responsible for the safety of data that they generate and handle; this must be kept secure at all times.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- They must avoid accidental breach by leaving a laptop unsecured and always 'lock' their computer whilst not in use, for example on a desktop, pressing the windows key and 'L'
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted, and password protected
- The device must be password protected
- The data must be securely deleted from the device once it has been transferred or its use is complete

E-Safety Policy

Communications

The school dissuades pupils from bringing mobile devices / phones into school; any pupils doing so must hand the device into the office for the day. Staff are not permitted to use their mobile phones during lessons or use their cameras. They must not send/receive personal emails or use any social media apps through the school network. It must only be used for school business.

- The official school email service is safe, secure and monitored.
- Users must immediately report any communication that is offensive, discriminatory, threatening or bullying in nature and must not respond to such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content using school email only. These communications may only take place on official (monitored) school systems
- Pupils will be taught to email responsibly, avoiding risks and being aware of hazards.
- Pupils should be taught about E-Safety issues, such as the risks attached to the sharing of personal details.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Communication technologies	Staff				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in lunch/break times	X							X
Taking images on personal devices				X				X
Taking images on school devices	X						X	
Use of school technical devices e.g. tablets, gaming devices	X						X	
Use of personal email addresses in school		X						X
Use of school email for personal emails	X					X		
Use of social media	X						X	
Use of blogs	X						X	

E-Safety Policy

Social Media - Protecting Professional Identity

Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Training to include acceptable use; social media risks, checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions

School staff should ensure that:

- No reference should be made in social media to 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 / academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss or personal information.

Unsuitable / Inappropriate actions

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abused images - The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	

	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
Online gaming (non-educational)					X	
Online gambling					X	
Online shopping / commerce					X	
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. Youtube			X			

Some internet activity is criminal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however activities which may be legal but inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the following activities would be inappropriate and users, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

Illegal - Child sexual abuse images, grooming, possession of gross pornographic image, material which incites criminally racist material or religious hatred.

Unacceptable – Pornography, threatening behaviour, promotion of extremism or terrorism, information which may be offensive to colleagues or the 'school'. Online gaming, gambling, promotion of physical violence or mental harm, using school systems to run a private business, creating or propagating computer viruses or other harmful files.

Responding to misuse

This guidance is 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 involve illegal or inappropriate activities.

E-Safety Policy

Illegal Incidents

If there is a suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (appendix) for responding to online safety incidents and report immediately to the police.

Other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

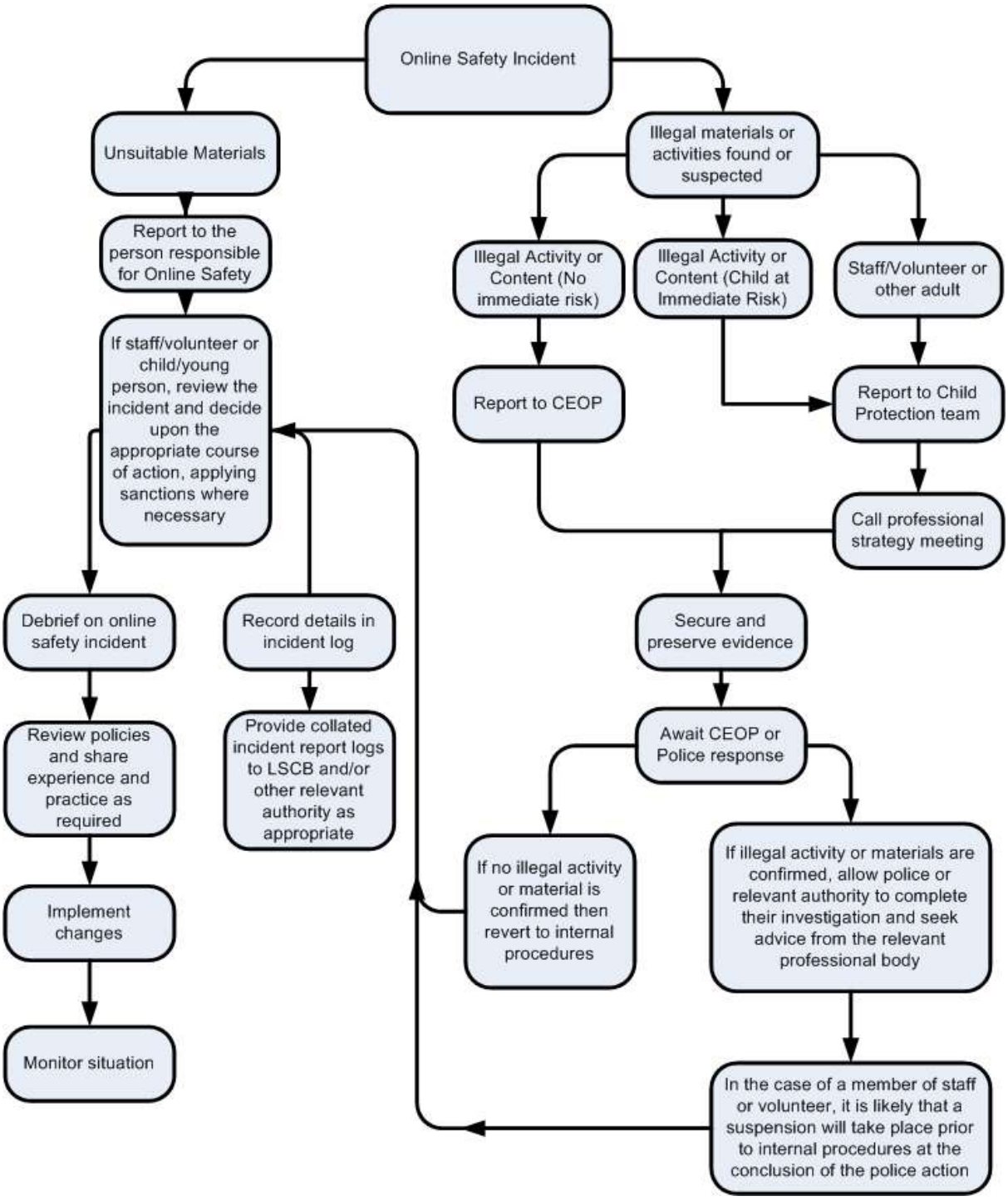
- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child 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
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the school and 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.

E-Safety Policy

School Actions / Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:



E-Safety Policy

Pupils

Incidents	Refer to class teacher	Refer to headteacher	Refer to police	Refer to Launch for filtering /	Inform parents / carers	Removal of network / internet rights	Warning
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x			
Unauthorised use of non-educational sites during lessons	X						
Unauthorised use of mobile phone / digital camera / other mobile device	X						
Unauthorised downloading or uploading of files	X						
Allowing others access to school network by sharing usernames and passwords	X						
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X		X		X	
Attempting to access or accessing the school / academy network, using the account of a member of staff		X		X		X	
Corrupting or destroying the data of other users		X				X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X	
Continued infringements of the above, following previous warnings or sanctions	X	X				X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X		X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X				X	

E-Safety Policy

Staff

Incidents	Refer to headteacherr	Refer to local authority / HR	Refer to police	Refer to LAUCNH for filtering / appropriate action erc	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)	X	X	X				
Unauthorised downloading / uploading of files							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account							
Careless use of personal data eg holding or transferring data in an insecure manner							
Deliberate actions to breach data protection or network security rules							
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software							
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature							
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils / 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's / 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							

E-Safety Policy

Reporting Log

Reporting Log Group	Date	Time	Incident	Action taken		Incident reported by	Signature
				What?	By whom?		

E-Safety Policy

User Agreement Policies UNDER REVIEW

Template KS1 Acceptable User Agreement Policy

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable 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.

Signed (child):……

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent / carer should be sufficient)

Signed (parent): ……..

E-Safety Policy

Template KS2 Acceptable User Agreement Policy

School Policy

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

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

Acceptable Use Policy Agreement

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.

For my own personal safety:

- I understand that the *school* will monitor my use of digital technology (using iPads, netbooks, internet)
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line (like names, where I live, where I go to school, my phone number etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report (tell an adult) any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school devices are used for school work and I will not use them for other reasons unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and stop other users from being able to carry out their work.
- I will not use the school devices for gaming, gambling, shopping, file sharing or video broadcasting (eg YouTube) unless I have permission from a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and will not access, copy, remove or change other peoples' work unless I have that person says I can.
- I will be polite and responsible when I communicate with others. I will not use rude or threatening words and I understand that other people will have different views to me.
- I will not take or share images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*

- I understand the risks and will not try to upload, download or access any materials which are illegal 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 get around the filtering / security systems in place to stop people viewing inappropriate things.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be dealt with in school. This may include: loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student / Pupil Acceptable Use Agreement Form

This form relates to the *student / pupil* Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school)
- I use my own equipment out of the school / academy in a way that is related to me being a member of this *school* eg communicating with other members of the school, accessing school email, website etc.

Name of Student / Pupil	
Group / Class	
Signed	
Date	

E-Safety Policy

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *pupils / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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 recognise the value of the use of ICT for enhancing learning and will ensure that pupils / pupils receive opportunities to gain from the use of ICT. 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 / academy* 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 (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are

published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- 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*:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school / academy* equipment. I will also follow any additional rules set by the *school / academy* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (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 / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not 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 School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / 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 / academy 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 school 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 the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy ICT equipment in school, but also applies to my use of school / academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	