Priors Field Primary School

Online Safety Policy

Policy Date: AUTUMN 2018

Approved by: FGB

To be reviewed: AUTUMN 2019

This Online Safety policy has been developed by:

- Headteacher
- Online Safety Co-ordinator
- Staff – including Teachers and Support Staff
- Governors
- Parents and Carers
- Community users

Consultation with the whole school and community has taken place through a range of formal and informal meetings.

The school has appointed an Online Safety Coordinator – Sue Bull

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on	
The implementation of this Online Safety policy will be monitored by the:	*Senior Leadership Team* *Online Safety Coordinator*
Monitoring will take place at regular intervals:	*Monthly Reports*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*FGB*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer,* *LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents and concerns
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the school community who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head Teachers 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 applies to cyber-bullying or other Online Safety incidents, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers to the searching for and of electronic devices and the deletion of data. The school will deal with such incidents within this policy and associated behaviour and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

- Governors are responsible for the approval and review of the Online Safety Policy, as well as the appointment of an Online Safety Governor

Head Teacher and Senior Leaders:

- The Head Teacher has a duty of care for ensuring the online safety of members of the school community, although the day to day responsibility will be delegated to the Online Safety Co-ordinator
- The Head Teacher/Senior Leadership Team (SLT) must be aware of the procedures to follow if a serious online safety allegation is made
- The Head Teacher/SLT are responsible for ensuring the Online Safety Co-ordinator and other relevant staff receive suitable training in their online safety roles
- The Head Teacher/SLT will ensure that there is a system in place for monitoring and support of those in school who carry out the internal online safety monitoring role. This provides a safety net and support
- The SLT will receive regular monitoring reports from the Online Safety Co-ordinator

Online Safety Co-ordinator:

- Leads the Online Safety Group
- Takes responsibility for online safety including leading, establishing and reviewing online safety policies etc
  Ensures all staff are aware of procedures to follow if an online safety incident occurs
- Provides training and advice for staff
  Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents
- Meets regularly with Online Safety Governor to discuss /review incident logs/ issues
- Attends relevant meeting of Governors
- Reports regularly to SLT

Network Manager:

Working alongside Warwickshire LA technicians, the Computing Leader is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online and LA safety technical requirements
  That users only access networks and devices through a properly enforced password protection policy
- The filtering policy is applied and updated on a regular basis (LA)
- That they keep up to date with online safety technical information
- That the use of the network / internet / Learning Platform / remote access / email is regularly monitored
- That monitoring software / systems are implemented and updated (in line with school policies)

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
  They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Head Teacher
- All digital communications with pupils / parents / carers is on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- 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
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities ensuring current policies are followed
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable and processes are followed for dealing with unsuitable material found in internet searches

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

Online Safety Group:

The Online Safety Group is a representative, consultative group with responsibility for issues regarding Online Safety including monitoring. The group will regularly report to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Co-ordinator with:

- The production / review / monitoring of the school Online Safety Policy / documents
- The production / review / monitoring of the school filtering policy
- Mapping /reviewing the online safety curricular provision – ensuring relevance and breadth
- Monitoring network / internet / incident logs
- Consulting stakeholders – including parents / carers / pupils about online safety provision
- Monitoring improvement actions identified through the 360 degree safe self-review tool

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Have a good understanding of research skills; avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Are expected to understand policies on use of mobile devices and digital cameras. They should understand policies on the taking / use of images and cyber-bullying
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that this Policy covers actions out of school (if related to membership of the school)

Parents / Carers:

- Parents / Carers play a crucial role in ensuring that their children understand how to use the internet / mobile devices in an appropriate way. The school will help parents understand these issues. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the use of digital images taken at school events and the website

Community Users:

- Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems

Policy Statements

Education – Pupils

The education of pupils in online safety is an essential part of the school's online safety provision. Children need the support of the school to recognise and avoid online safety risk. Online safety must be a pivotal in all areas of the curriculum and staff should clearly reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progressive.

- Planned online safety objectives should be met as part of Computing / PHSE
- Key online safety messages should be reinforced through assemblies
- Pupils should be taught in all curricular lessons to be critically aware of the materials / content they access on-line and to validate the accuracy of information
- Pupils should understand the pupil Acceptable Use Agreement and adopt safe / responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, pupils should use sites checked for their use and processes are in place for dealing with unsuitable material

Education – Parents / Carers

Many parents and carers are unaware of online safety risks and issues. Parents may underestimate how often children and young people come across potentially harmful material and may be unsure how to respond.
The school will therefore seek to provide information to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites / publications

Education – The Wider Community

The school will provide opportunities for local members of the community to gain from the school's online safety knowledge and experience through the following:

- Reference to relevant websites/ publications

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff; regularly updated and reinforced An audit of the online safety training needs of all staff will be carried out regularly
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements
- The Online Safety Co-ordinator will receive regular updates through attendance at external training events
- This Online Safety Policy and its updates will be presented to and discussed by staff
- The Online Safety Co-ordinator will provide advice / guidance / training to individuals as required

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 – infrastructure / equipment, filtering and monitoring

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. It will also need to ensure that people named in the above sections carry out their online safety responsibilities:

Equipment and software

The school uses the Warwickshire image on all computers including laptops

- All users will have clearly defined access rights to school technical systems and devices
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All equipment is protectively marked and logged
- No hardware or software will be installed without permission from senior management
- The use of personal ICT equipment in school is subject to electrical testing and permission from senior management
- Access to the school wireless network is subject to permission from senior management
- School related ICT/communication out of school should be accessed through the Learning Platform (Welearn365)
- Disposal of computer hardware should only be through approved County professional services

Managing filtering

- The school works in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible
- The Online Safety Coordinator ensures that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

Passwords and GDPR (Data Security)

- Passwords are changed regularly, not written down, saved or shared with anyone else
- Passwords should include upper and lower case letters as well as numbers
- Use secure remote access whenever possible through learning platform (Welearn365)
- Encryption of removable data – It is a legal requirement of the Data Protection Act 1988 to protect and secure personal data - only use password protected USB drives
- If secure remote access is not possible, users must only remove or copy personal or sensitive data if the storage media, portable or media device is encrypted and is transported securely for storage in a secure location
- Computers should not be left logged on or unattended at any time
- Laptops/mobile devices should be shut down and locked securely when unattended
- Staff should not allow others to use their login details
- Staff, governors and children have access to the learning platform (Welearn365)
- Reception class use a class log in
- Year 1 – passwords are created and are given out when first using the learning platform (Welearn365) and are changed to personal passwords in Year 2 and Key Stage 2
- Portable media may not be used without specific permission and a virus check
- Any administrator passwords for the school ICT system, used by the ICT Manager must also be available to the Headteacher and kept in the school safe

- Guest log ins are available for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly
- Passwords are changed regularly (see passwords and data security policies)
- Virus protection is installed on all computers and laptops and is updated by ICTDS
- The school uses the Warwickshire Broadband with its firewall and filters
- The school provides an additional level of protection through its deployment of monitoring software in partnership with Warwickshire ICT Development Service. This software monitors text appearing on the screen and keyboard input, identifying the use of words that are included on a list of ‘banned words’. The software captures the screen, identifying machine and user details so appropriate action can be taken. Any online safety incidents are reported in weekly business staff meetings and full governors meetings

E-mail

- Pupils and staff can only use approved e-mail accounts on the school system accessed through the Warwickshire Learning Platform (Welearn365) for school related activities
- Pupils are advised to tell a teacher immediately if they receive offensive e-mail
- Pupils are advised that they must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Use of words included in the monitoring software ‘banned’ list are detected, logged and monitored by SLT
- Pupils are advised that any e-mail sent to an external organisation should be written carefully, politely and sensibly and authorised before sending
- Pupils are made aware that the forwarding of chain letters is not permitted

Authorising Internet access

- All staff/volunteers read and sign the Acceptable Use Policy - Staff and Volunteers, before using any school ICT resource. (See appendix 2)
- At Key Stage 1, access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials
- Parents sign the Online Safety agreement form for parents of primary aged children. (See appendix 3) as part of Reception induction or when their children join the school
- Children s parents/carers sign the online safety agreement form for primary school pupils (See appendix 4 Key Stage 2, 4a Key Stage 1). These are countersigned by parents who are asked to help reinforce our rules for online and ICT use in school and at home (See appendix 4a for both Key Stage 1 & 2 and appendix 5, Key Sage 1 rules and appendix 6 for Key Stage 2 rules)

Mobile Technologies

There may be school owned mobile devices which have capability to access the internet/email and cloud based services. Their use must be educational and in line with all our related policies. Teaching about the safe and appropriate use of mobile technologies are an integral part of the school’s online safety education programme.

- Mobile technology is only used during lessons or formal school time when authorized. All school mobile devices are kept locked in the server room when not in use and at the end of day. Class sets of ipads must be signed in and out and logged with users and must not be separated
- Staff must not use their own mobile phone/ device where contact with pupils or a parent is required
- Staff must not take or store images of children on their mobile devices
- Only school devices can be used to take images/videos and must be cleared every day
- Only school mobile devices/phones are used during educational visits, including residential trips
- Staff must switch off their mobile phones during lessons or any contact with pupils in the classroom or anywhere else in school and be safely secured away with all personal possessions
- Mobile phones may only be accessed with NO children present in the safety of the staffroom or where there are no children present
- All mobile devices taken out of school must be signed out and signed back in (See folder in office)

The school allows:

	School Devices			Personal Devices		
	School owned single user	**School owned multiple users**		**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes		No	Yes (See mobile devices)	Yes (Only when agreed)
Full network access	Yes	Yes		No	No	No
Internet only				No	Yes	No (Only Guest log in)

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. The school will inform and educate users about these risks to reduce the likelihood of the potential for harm:

- When using digital video/images, staff should inform and educate 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
- Written permission from parents or carers will be obtained before photographs/videos of pupils are published on the school website / social media / local press (See appendix 1)
- The school will issue guidance specific to occasions regarding parents creating photos and videos of their children at school events
- Staff are allowed to take digital / video images, but must follow school policies concerning the sharing, distribution and publication of those images. Images should only be taken on school equipment
- Care should be taken when taking digital / video images; pupils must be appropriately dressed and only participating in suitable activities
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs of pupils published on the website will be selected carefully and comply with good practice guidance. Pupils' full names will not be used on a website or in in association with photographs

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR 2016) – please also see Priors Field Information Security Policy and Priors Field Data Protection Policy.

Staff must at all times realise that they are personally responsible for the safety of data that they generate and handle; this must be kept secure at all times. They must avoid accidental breach by leaving desktops/laptops unsecured and always 'lock' their devices whilst not in use.

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
- Pupils will be taught to email responsibly, avoiding risks and being aware of hazards

Social Media - Protecting Professional Identity

The school provides the following measures to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

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 relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for administration and monitoring– involving at least two members of staff
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Monitoring of Public Social Media:

- The school will monitor social media postings and take action accordingly

Unsuitable / Inappropriate activities

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'. On line 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 incidents of 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.

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 (see page 11) for responding to online safety incidents and report immediately to the police.

Other Incidents

There may be times when infringements of the policy could occur through careless, irresponsible or, rarely, deliberate misuse.

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

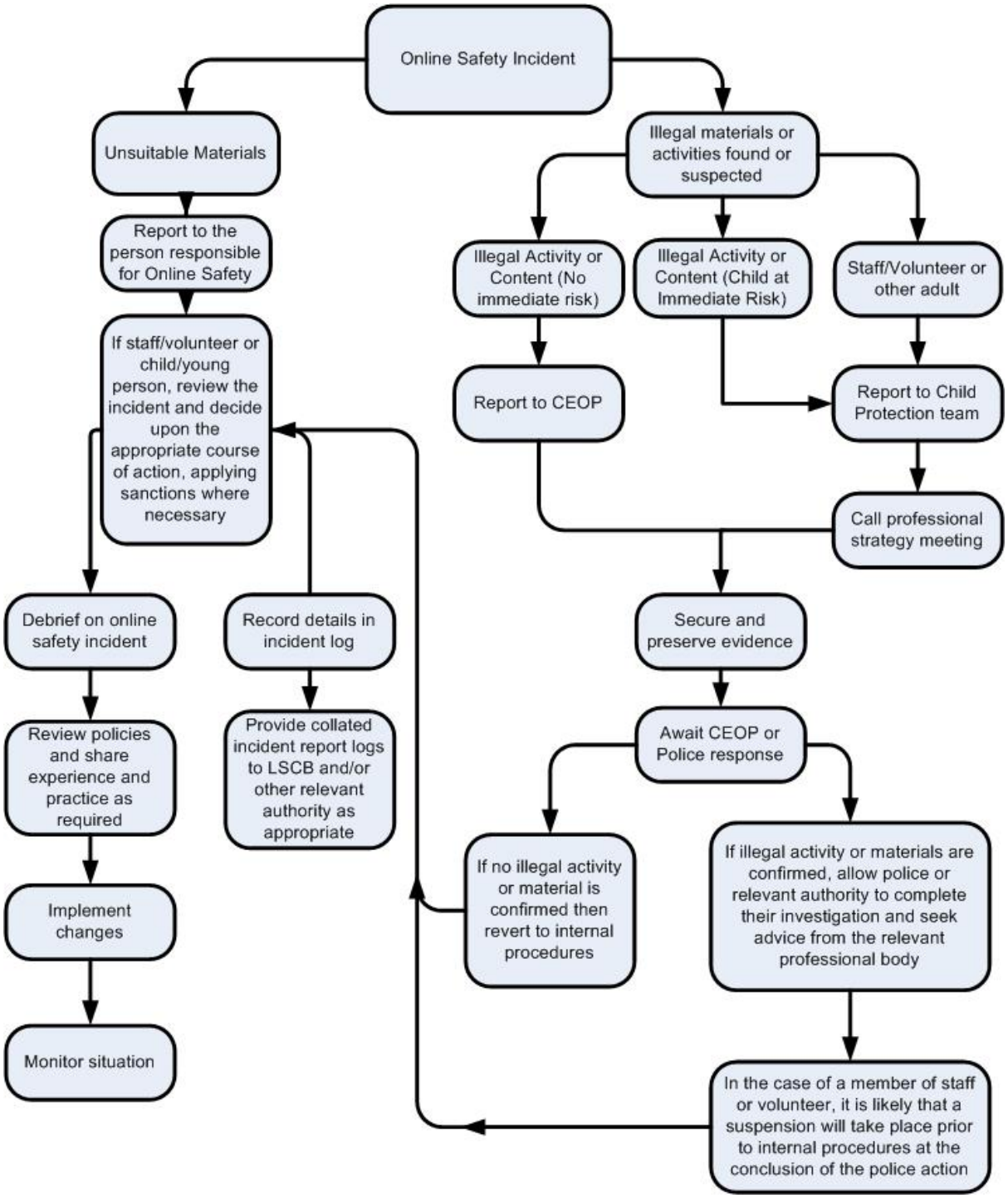
- Have more than one senior member of staff involved in this process. This is to protect individuals if accusations are subsequently reported
- Conduct the procedure using a designated computer which is not used by young people and can be taken off site by the police, should the need arise
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but that 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. 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)
- Once 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:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement

- If content being reviewed includes images of Child abuse then 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
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question. Any change to its state may hinder a later police investigation.

It is important that these steps are taken to provide an evidence trail for the school /police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with inappropriate incidents rather than illegal misuse. It is important that any incidents are dealt as soon as possible. Incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.



Appendix 1

Consent Form for the recording and use of Images

Name of Pupil …….. Year Group ……..

Dear Parent/Carer

During the course of the school year, we may sometimes wish to take photographs or video recordings of children within school or on school trips, either for our own records, for use as part of our learning curriculum or for inclusion in our promotional material such as the school prospectus and our website.

The school may also invite an external photographer to the school each year to take official school photographs and may invite the media in to take photographs of pupils engaged in school activities or events for publication.

To comply with the General Data Protection Regulation, we need to ask your consent before the school record any images of your child. In view of this, please read the statements below, complete and return this form to school within the next 7 days**.**

This table sets out the various reasons for taking, and making use of, images of your child and we should be grateful if you would indicate whether or not you give consent for use in these circumstances. By indicating 'YES', you are confirming that you consent to your child's personal data being shared for those purposes and/or with the named third parties:

1.	For official school photographs, with images taken by Braiswick Photographic Co Ltd and available for purchase by parents, and held by the school for identification purposes with names attached.	YES/NO
2.	For use on internal school displays and educational use in school, on the school's website and in parental information such as school newsletters.	YES/NO
3.	I consent to my child taking part in video conferencing as part of the curriculum using our secured educational broadband network to ensure quality service and security.	YES/NO

4.	I consent to images of my child engaged in school activities or events during school hours appearing in external media organisations, such as Kenilworth Weekly News. First names only maybe attached to any images.	YES/NO

This form is valid for the period of time your child attends this school and will automatically expire after this time.

Please note, you have the right to withdraw or change your consent at any time by giving the school written notice and completing a new consent form. You can notify us of your consent withdrawal in writing by contacting admin2605@welearn365.com

Signature ……..

Name…….

Relationship to child ……

Address

……..

……..

Telephone number ……

Date ……

Appendix 2

Acceptable Use Policy Agreement (Staff and Volunteers)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. mobile devices, 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 digital technology 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 social networking sites in school in accordance with the school's policies.
- I will only communicate with 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 (laptops / tablets / 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 equipment. I will also follow any additional rules set by the school 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 only use my professional email account for school business
- 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 not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school. I will not disable or cause any damage to school 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 Personal Data Policy and Information Security 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 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 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 digital technology equipment in school, but also applies to my use of school 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.

- 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 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 digital technology 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: .....

Appendix 3

Online Safety Agreement Form
For Parents of Primary Aged Children

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter / son to have access to use the Internet and other ICT facilities at school.

I understand that my daughter / son will sign an online safety agreement form and that they will be taught the 'rules for responsible online and ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered and monitored service, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent / guardian signature: _____
Date: ___/___/___

This form is valid for the period of the time your child attends this school and will automatically expire after this time.

Appendix 4

Online Safety Agreement Form
For Primary School Pupils

Key Stage 2
Keeping Safe:
Stop, think, before you click!

Pupil name: _____

I have read the school's rules for responsible online and ICT use. My teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, mobile devices and other ICT in a safe and responsible way. I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, they may contact my parent / carer.

Pupil's signature _____

Date: ___/___/___

This form is valid for the period of the time I attend this school and will automatically expire after this time.

Appendix 4a

Dear Parent/Carer

ICT including the internet, email and mobile technologies etc. has become an important part of learning in school. We expect all children to be safe and responsible when using any ICT.

In class we have discussed and completed work on our rules for responsible use of the internet and ICT use. To help us reinforce this lifelong skill please could you take the time to read and discuss these safety rules with your child and return their agreement form together with this as soon as possible. If you have any concerns or would like clarification please do not hesitate to contact the school.

Parent / Carer Signature

We have discussed this and ……(child name) agrees to follow the safety rules and to support the safe use of ICT in school.

Sanctions for misuse are outlined in our behaviour policy.

Parent/Carer Signature……..

Class……. Date……

Please return with Online Safety agreement form signed by your child.

Online Safety Agreement Form

For Primary School Pupils

Key Stage 1

Keeping Safe:
Stop, think, before you click!

Pupil name: _____

My teacher has explained the school's rules for responsible online and ICT use to me.

I understand these rules are there to help keep me safe, as well as my family and friends.

I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, mobile devices and other ICT in a safe and responsible way. I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, they may contact my parent / carer.

Pupil's signature _____

Date: ___/___/___

This form is valid until I move into year 3 and will be updated at that time.

Appendix 5

Keeping Safe:
Stop, think, before you **click!**

Rules for Online and ICT use
Key Stage 1

We only use the Internet when a trusted adult is with us

We only click on icons and links when we know what they do or when our teacher or parent/carer has asked us to

We never tell anyone our personal information (name, address, phone number, school or passwords)

We are always polite and show respect when communicating with others

We always tell a trusted adult if we find something that we do not understand or that upsets us

These rules will keep everyone safe and help us to be fair to others.

Appendix 6

Keeping Safe:
Stop, think, before you **click!**

Rules for Online and ICT use
Key Stage 2

These rules will keep everyone safe and help us to be fair to others

- I will only use ICT in school for school purposes.
- I accept that I am responsible for all activity carried out under my user name.
- I will always take care of ICT equipment and leave it as I found it.
- I will only open or delete my own files and I will not look or change other people's files without their permission.
- I will not bring files into school without permission.
- I will ask permission from a member of staff or trusted adult before using the Internet.
- I will only message/e-mail people I know with the permission of a member of staff or trusted adult.
- The messages I send, or information I upload, will always be polite and respectful.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any members of our school community.
- I will not tell other people my ICT passwords or give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless member of staff or trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, carer or member or staff has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a member of staff/responsible adult.
- I understand that everything that I create or look at leaves a 'digital footprint' that can be traced.
- I am aware that some website and social networks have age restrictions which I will respect.