Online Safety Policy

Written By: Tim Lewington, Online Safety Leader

Ratified By Governors

Live life in all its fullness (John 10:10)

1. Introduction

1.1 Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education including governors, senior leaders, classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

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

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1.1 Development and Review of this Policy

This policy has been developed by the Online Safety working party made up of:

- Deputy Headteacher
- ICT/Online safety leader
- Governing Board
- Parents and Carers

1.2 Schedule for Development / Monitoring / Review

This Online safety policy was approved by the Governors' Performance and Standards Committee on:	May 2021
The implementation of this Online safety policy will be monitored by:	Jenny Mitchell-Hilton Deputy Headteacher Tim Lewington Online safety/ICT Leader Online safety Working Party
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:	Summer 2024
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Margaret Pollard (School's Designated Safeguarding Lead) Warwickshire MASH if appropriate ICT Development Service Warwickshire Police

The school will monitor the impact of the policy using:

- Behaviour logs of reported incidents where appropriate
- Headteacher log of concerns raised by parents
- Monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

1.3 Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) 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 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 online safety incidents covered by this policy, which may take place outside the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

2. Roles and Responsibilities

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

2.1 Governors:

Governors are responsible for the approval of this policy and for reviewing the effectiveness of it. This will be carried out by a member of the Governing Body who has taken on the role of online safety governor. The role of the online safety governor will include:

- regular meetings with the online safety leader
- regular monitoring of online safety incident logs
- reporting to relevant governors / committee / meeting

2.2 Headteacher and Senior Leaders:

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the online safety leader.

The headteacher and the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on P16 dealing with online safety incidents)

The headteacher is responsible for ensuring that the online safety leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The senior leadership team will receive regular monitoring reports from the online safety leader.

2.3 Online safety leader:

- leads the online safety champions student/governor/teacher/parent group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body

- liaises with Local Authority technical support
- reports online safety incidents to the headteacher to decide an appropriate course of action
- meets regularly with the online safety governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior LeadershipTeam
- Keeps a prominent advisory display board up to date in school

Investigation into incidents will be dealt with by the online safety leader, where relevant, with sanctions being the responsibility of the headteacher.

2.4 Technical Staff

The school has a managed ICT service provided by Warwickshire ICT Development Service. It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school's online safety policy and procedures.

Technical Staff in school, ICT Subject Leader and Warwickshire ICTDS are responsible for ensuring:

- that each school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network, internet, Welearn365, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the headteacher or online safety leader for investigation, possible action and sanction
- that monitoring software and systems are implemented and updated as agreed in school policies

2.5 Teaching and non-teaching staff

Teaching and non-teaching staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school's online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement (appendix 1).
- they report any suspected misuse or problem to the headteacher or online safety leader for investigation, possible action and sanction
- all digital communications with pupils and parents/carers should be 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 and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- 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 for dealing with any unsuitable material that is found in internet searches

2.6. Designated Safeguarding Leads

The designated persons for child protection at each school should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding 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

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

2.7 Digital Heroes Group

The online safety group provides a consultative group that has wide representation from across the school, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. The group will meet regularly and be responsible for regular reporting to the Performance and Standards Governing Body Committee.

Members of the Digital Heroes Group will assist the online safety leader with:

- the production, review and monitoring of the school online safety policy and accompanying documents.
- the production, review and monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety curricular provision - ensuring relevance, breadth and progression
- monitoring network, internet and incident logs
- consulting stakeholders - including parents/carers and the pupils about the online safety provision

Membership of the Digital Heroes group should include representation from staff, pupils and parents/carers where possible.

2.8 Pupils

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy (appendix 2).
- have a good understanding of research skills and the need to 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
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and the use of images and on cyber-bullying.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

2.9 Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Our school takes every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Welearn365 and information about local and national online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of Welearn365
- their children's personal devices in the school (where this is allowed)

2.10 Community Users

Community users who access school systems as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement (appendix 3) before being provided with access to school systems including the wifi.

3. Policy Statements

3.1 Education - Pupils

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 online safety is therefore an essential part of our school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing and PHSE lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement (appendix 2) and encouraged to adopt safe and 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, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children visit.

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, medicines, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that ICTDS (or other relevant designated person) 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.

3.2 Education – Parents and Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website, Welearn365
- Parents /information evenings and workshops
- High profile events and campaigns e.g. Safer Internet Day, Anti-Bullying Week.
- Reference to relevant websites and publications e.g. www.saferinternet.org.uk/ www.childnet.com/parents-and-carers www.thinkuknow.co.uk

3.3 Education – The wider community

The school will provide opportunities for local community groups to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- online safety messages targeted towards grandparents and other relatives as well as parents.
- The school's website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, childminders, voluntary organisations to enhance their online safety provision.

Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

3.4 Education and Training – Staff

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. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy and Acceptable Use Agreements.
- The online safety leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.

- The Online safety Co-ordinator will provide advice, guidance and training to individuals as required.

3.5 Training –Governors

Governors should complete online safety training. In addition they may be offered:

- Training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in school training/information sessions for staff or parents, including assemblies and lessons.

3.6 Technical – Infrastructure and equipment filtering and monitoring

The school will be responsible for ensuring that the school network and Welearn365 is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- The school ICT system will be managed in ways that ensure that it meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of each school's 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 ICT systems and devices.
- All users will be provided with a username and secure password by ICTDS who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password when prompted in accordance with LA password policy. Staff teaching younger children may choose to use group or class log-ons and passwords but need to be aware of the associated risks.
- Supply teachers should use a guest user name provided by the office which can be tracked according to the hours worked.
- The administrator passwords for the ICT system must also be available to the senior leadership team and kept in a secure place
- The headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.)
- The school maintains and supports the managed filtering service by Warwickshire ICTDS.
- Any filtering issues should be reported immediately to ICTDS via the online safety leader or headteacher
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users - staff/pupils etc).
- Requests from staff for sites to be removed from the filtered list will be considered by two people from SLT. If the request is agreed, this action will be made via email and recorded. Logs of such actions shall be reviewed regularly by the online safety group.
- The local authority's technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the online safety leader or headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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 anti-virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) on to the school systems.
- An agreed policy is in place regarding the extent of personal use that staff are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to download executable files and install programs on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Staff are requested not to use removable media (e.g. memory sticks, CDs/DVDs).

4. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. 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 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital or video images.
- 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 (Appendix 4 Use of images guidance). Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- 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 (Appendix 4 Use of images guidance).

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- A minimum of 3 children to be present in any single photograph.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/press
- Pupils' work can only be published with the permission of the pupil and parents or carers.

5. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- 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 (many memory sticks and other mobile devices cannot be password protected)
- the device must offer approved anti-virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

6. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff & other adults				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		✔						✔
Use of mobile phones in lessons				✔				✔
Use of mobile phones in social time	✔							✔
Taking photos on mobile phones / cameras			✔					✔
Use of other mobile devices eg tablets, gaming devices		✔				✔		
Use of personal email addresses in school, or on school network			✔					✔
Use of school email for personal emails				✔				✔
Use of messaging apps		✔						✔
Use of social media			✔					✔
Use of blogs		✔				✔		

When using communication technologies the school considers the following as good practice:

- The official Welearn365 email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the Welearn365 email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person - in accordance with the school policy - the receipt of any communication that makes them feel

uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents/carers must be professional in tone and content**.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used in the Early Years, while pupils at Year 1 and above will be provided with individual Welearn365 email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

8. Social Media – Protecting Professional Identity

All schools, and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber-bully, 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 social media policy and staff code of conduct details specific requirements and guidelines regarding staff's use of social media.

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 limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- In line with Staff Code of Conduct, staff will declare links (to the headteacher) on social media with parents at the school.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- The headteacher provides monthly monitoring of the school's social media activity in order to check it's appropriateness and coverage.

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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the online safety committee to ensure compliance with the Social Media and Data Protection Policies and code of conduct.

9. Unsuitable or Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal 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 a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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 **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:**	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✔
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✔
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✔
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					✔
Pornography				✔	
Promotion of any kind of discrimination				✔	
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				✔	
Using school systems to run a private business				✔	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✔	
Infringing copyright				✔	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✔	
Creating or propagating computer viruses or other harmful files				✔	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				✔	
On-line gaming (educational)	✔				

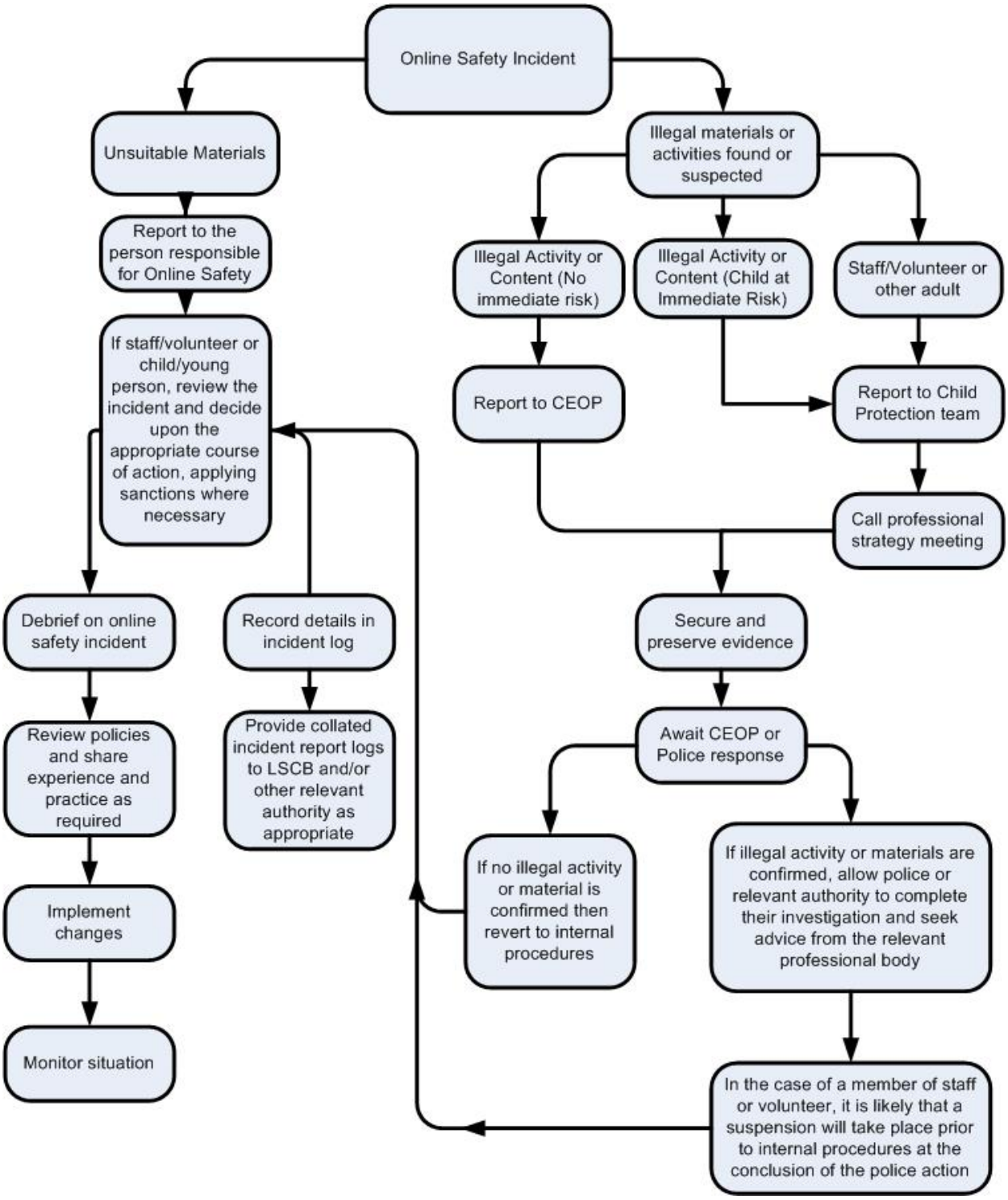
On-line gaming (non educational)		✔			
On-line gambling				✔	
On-line shopping / commerce		✔			
File sharing	✔				
Use of social media			✔		
Use of messaging apps			✔		
Use of video broadcasting eg Youtube	✔				

10. Responding to incidents or misuse

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

10.1 Illegal incidents

If there is any 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 below for responding to online safety incidents and report immediately to the police.



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 of 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.

10.2 School actions and 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:

Pupil Incidents	Actions / Sanctions								
	Refer to Class Teacher	Refer to Online safety leader	Refer to Headteacher	Refer to Police	Refer to ICTDS for action re filtering/security etc	Inform parents/ carers	Removal of network/internet access rights	Warning	Further sanction 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 mobile device		✔	✔			✔		✔	
Unauthorised use of social media / messaging apps / personal email		✔	✔		✔	✔	✔	✔	
Unauthorised downloading or uploading of files		✔	✔		✔	✔	✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔					✔	✔	
Attempting to access or accessing the school network, using another pupil's account		✔	✔			✔	✔	✔	
Attempting to access or accessing the school network, using the account of a member of staff		✔	✔		✔	✔	✔		✔
Corrupting or destroying the data of other users		✔	✔		✔	✔	✔		✔
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✔	✔			✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions		✔	✔			✔	✔		✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✔	✔			✔	✔		✔
Using proxy sites or other means to subvert the school's filtering system		✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material and failing to report the incident		✔	✔		✔	✔	✔		
Deliberately accessing or trying to access offensive or pornographic material		✔	✔	✔	✔	✔	✔		✔

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✔	✔	✔		✔	✔		

Staff Incidents

Actions / Sanctions

	Refer to Headteacher	Refer to Local Authority/Governors/HR	Refer to Police	Refer to ICTDS for action re filtering/security etc	Warning	Possible Disciplinary Action	Possible suspension/ dismissal
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔			✔	✔
Inappropriate personal use of the internet / social media / personal email	✔			✔	✔	✔	
Unauthorised downloading or uploading of files	✔			✔	✔		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✔			✔	✔		
Careless use of personal data eg holding or transferring data in an insecure manner	✔				✔	✔	
Deliberate actions to breach data protection or network security rules	✔	✔		✔		✔	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✔		✔	✔		✔	✔
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✔	✔				✔	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	✔	✔		✔		✔	✔
Actions which could compromise the staff member's professional standing	✔	✔			✔	✔	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔	✔			✔	✔	

Using proxy sites or other means to subvert the school's / 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	✔	✔				✔	

11. Acknowledgements

This policy is based on the Template policies by SWGFL, who would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online safety Policy Template and of the 360 degree safe Online safety Self Review Tool:

- Members of the SWGfL Online safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Appendix 1 Staff Acceptable Use Agreement

Kineton C of E Primary School Acceptable Internet Use Policy

Staff and volunteers

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 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 technology in their everyday work.

The computer system is owned by the school, and may be used by students to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's Online Safety and Social Media policies and Code of Conduct have been drawn up to protect all parties – the pupils, the staff, the school and its community. To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff and volunteers should consult the school's Online safety and Social Media policies and Code of Conduct for further information and clarification.

I agree that I will:

- only use, move and share personal data securely whether in school, taken off the school premises or accessed remotely.
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use school equipment to take photographs and videos
- only store photos on the school network and Gdrive, rather than personal devices
- ensure that any photos published online only include images of pupils who have parental permission to appear publically, are in groups of three or more and are only identified by first name if necessary (never with surname).
- store cameras out of sight and safely
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils

- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the Online safety Leader or Headteacher
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
- pornography (including child pornography), promoting discrimination of any kind, violence or bullying, racial or religious hatred promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative
- publish images of individual pupils online or with their name

- I know that anything I share online may be monitored.

- I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

- I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

- I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

- I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used to ensure the school's policies are being followed.

I have read, understood and agree with Acceptable Use Policy.

Signed: …… Capitals: …… Date: ……

Kineton C of E Primary School
Safe Internet Use Policy
Foundation Stage and Key Stage 1 Pupils

In school the internet is used to help us with our learning. These rules will keep you safe and help us be fair and respectful to others.

" When you **click**, **click**, **click**, you need to **think**, **think**, **think** and **tell** a trusted **grown-up**."

Kineton C of E Primary School

To keep myself safe I will:

- Only use the internet when an adult is with me.

- Click on the buttons or links when I know what they do.

- Always ask if I get lost on the internet.

- Only use my personal school e-mail in school.

- Only send polite and friendly emails to people that I know.

- Tell a teacher straight away if I get a message or see something I don't like.

- Keep my password secret from my friends.

- Do not tell people about myself online (my name, phone number anything about my home, family or pets)

Acceptable Internet Use Policy

Key Stage 2 Pupils

In school the internet is used to help us with our learning. These rules will keep you safe and help us be fair and respectful to others.

"Report, block, tell a grown-up that you trust!"

To keep myself protected online I will:

- only access the system with **my own login** and **password** which I will ALWAYS keep secret.
- not bring in **portable data storage** e.g. memory sticks, disks from home.
- Use the internet with an **adult present** in the same room.
- make sure all **messages** I send are **respectful**.
- show a **responsible adult** any content that makes me feel unsafe or uncomfortable. I understand this will be **confidential** and will help protect other pupils and myself.
- **not reply** to any nasty message or anything which makes me feel uncomfortable
- only use my personal Warwickshire **school email address**, provided by school, in school for school purposes.
- not use **internet chat rooms or social networking** sites in school. Minimum age for most social-networks is 13 years old.
- always keep my **personal details private** (my name, family information, journey to school, my pets and hobbies are all examples of personal details).
- always check with a responsible adult before I share **images** of myself or others.
- never arrange to **meet** anyone I don't know.
- never **share** anything online. I know that once I share it is completely out of my control and may be used by others in a way I did not mean.
- the school may **check** my computer files and will monitor the internet sites I visit.
- I WILL BE IN SERIOUS TROUBLE AND REPORTED TO THE HEADTEACHER IF ANY SITE I VISIT IS THOUGHT TO BE UNSUITABLE FOR MY AGE.

Appendix 3 Community User Acceptable Use Agreement

Kineton C of E Primary School
Acceptable Internet Use Policy
Community Users

The computer system is owned by the school, and may be used by students to further their education and by staff to enhance their professional activities including teaching, research, administration and management The school's Online safety and Social Media policies and Codes of Conduct have been drawn up to protect all parties – the pupils, the staff, the school and its community.

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school / academy:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person (Mrs Barritt, Online safety Leader or Margaret Pollard, Headteacher).
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without

permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.

- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy 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 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 if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

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.

I have read, understood and agree with the Acceptable Use Policy.

Signed: …….. Capitals: …….. Date: ……

Appendix 4 Use of images Guidance

Kineton Primary School
Guidance on the use of images – Update June 2017

(Based on Use of Images Guidance for children and young people in Warwickshire December 2014)

- Taking pictures and videos of children and young people's achievements and activities is a wonderful way of capturing memories and promoting successes but consideration needs to be given as to how those images may be used.
- As photographic images can be misused through modification or distribution via the internet a number of issues must be considered before decisions are made to use such images and how to use them.
- This document aims to minimise the risk of misuse of images and to ensure that individuals' safety and welfare are not compromised.

Taking Photographs

- A clear purpose is needed for the photograph or video.
- For practical and safeguarding purposes, the school will seek written consent from a parent, guardian or carer for all pupils. An explanation of the different ways in which the pictures may be used will be provided and they will be given the choice to opt out. **Consent will be sought as part of the school enrolment process when a child joins the school, and in line with GDPR requirements. Parents will be given the option to withdraw or amend their consent at any time.**
- **A list of photographic consent for pupils will be shared with all staff and updates provided as required.**
- Adults working in school will be asked for their consent as to whether they give permission for their photograph to be taken and published. Permission will be sought at the beginning of their employment and remain in place unless withdrawn. (see Appendix D).
- **Images should only be taken using equipment which is provided by the school to record and store those images. The personal equipment of staff should not be used for such purposes including mobile phones except in the circumstances detailed below.** Equipment used to store images should always remain in the establishment. The headteacher and governors reserve the right to check any images taken using school equipment.
- **For the purposes of Tweeting or putting photographs on Facebook, images may be taken on a mobile phone but should be immediately deleted in order to protect both the children and member of staff.**
- **Staff taking photographs using personal devices for this purpose consent to be subject to spot checks of their devices.**
- Camera equipment used to record official off-site school/setting activities, e.g. displays/outings, should only be used by authorised staff and volunteers and should be returned to the establishment or approved secure place immediately after the activity.

- It is advisable that students requiring images for work placement portfolios only use images provided by the setting, school or organisation and that where appropriate parental consent has been sought if individual pupils are identifiable in them.
- When taking images at an event attended by large crowds, such as a sports event, this is regarded as a public area and so permission is not required from everyone in a crowd shot. People in the foreground are also considered to be in a public area. However, it is recommended that photographers address those within earshot, stating where the photograph may be published and giving them the opportunity to move away
- If there are child protection concerns, these should be discussed with Children's Social Care services in order to ascertain whether it is appropriate for a child to appear in a production rather than banning the use of video or taking of photographs and drawing further attention to this.

Storage and Security of Photos

- Images should not be stored on personal devices. Instead, photos should be stored on the school network in the Photos folder. This will be regularly reviewed so images of pupils no longer in school are deleted. Photos should not be kept for longer than necessary.
- Cameras should be stored out of sight when not in use, no one is in the classroom and out of school hours.
- Images of pupils who have left the school should be deleted unless these images are being used for publicity purposes e.g. in the school prospectus or website.

Use of Images

- When publishing the images e.g. on the school website, Facebook or Twitter, individual shots should NOT be used. Children should be shot in groups of a minimum of three.
- When using group shots refer to the group as a whole. It should not usually be necessary to use a child's name or age.
- When using digital 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- When a story relates specifically to the success or achievement of an individual or small group of children, it may be appropriate to name those children but you should ensure that you have the appropriate consent. However, first names may only be used with an initial if there is more than one child in school with that name , e.g. "John S. in Year 4" alongside the image of a child.
- Personal details of children such as e-mail addresses, home addresses and telephone numbers should never be revealed.
- Consider the subject matter in use. If the text is something controversial e.g. bullying then an image from a Stockphoto or other generic image sites should be used.
- If any member of staff or volunteer notices any possible misuses of images, this should be reported immediately to the designated safeguarding lead using the green form 'Logging a concern about a child's welfare and safety' available in the staffroom.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect

everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital or video images. At the beginning of an event, parents and carers will be asked not to place any recording or images on social networking sites, such as Facebook or YouTube.

Copyright

- If the photographer is a member of staff or volunteer in an organisation on whose behalf photographs/videos are taken, she/he will be acting on behalf of the organisation and the organisation will own the copyright.
- If the photographer is an employee of a company instructed to take photographs/videos by an organisation, the photographer will be acting on behalf of his/her employer and the company the photographer works for will own the copyright