



Online safety Policy

Chair of Governors	Mr F Maguire
Headteacher	Mrs L Shelford
Date adopted: October 2022	Review Date: October 2024

The caring path to achievement, reflecting the values of Christ.

Aims of Policy

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Standards Committee, who receive regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online safety Governor. The role of the Online safety Governor will include:

- Meetings with the Computing Subject Leader
- Monitoring of online safety includes logs
- Monitoring of filtering/change control logs
- Reporting to relevant Governors Committee

Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, through the day to day responsibility for online safety will be delegated to the Computing Subject Leader.
- The Headteacher (Deputy Safeguarding Lead), Head of Safeguarding (Safeguarding Lead) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Computing Subject 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 Headteacher will ensure that there is a system in place to allow the monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher will receive regular monitoring updates from the Computing Subject Leader.

Computing Subject Leader:

- 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.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. Meets with Online safety Governor to discuss current issues, review incidents logs and filtering/change control logs.
- Reports regularly to the Headteacher.

- The Online safety Subject Leader will review and update the policy annually in partnership with our IT provider, the Safeguarding Lead, the School Council and the School Business Manager.

Online safety Group:

- The online safety group consists of Sue Swift (safeguarding leader), David Atkinson (computing subject leader), Mandy Pierce (Business Manager), Daniel Foster (IT support), Donna Barker (Pastoral manager) and Bethany Donovan (local PCSO).
- Meets at least once per term.
- Monitors the impact of online safety education and recommends any changes necessary.
- Raises new initiatives (e.g. safer internet day, and the introduction of an online code of conduct created by pupils)
- Assists in the monitoring and review of policies relating to online safety.
- Arranges regular parents' information events and ensures that the information and advice we make available for parents is relevant and appropriate.

Technical Staff:

The Computing Subject Leader is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required online safety technical requirements and any Local Authority/other relevant body Online safety Policy/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.
- Filtering is applied and updated on a regular basis.
- 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 /remote access/e-mails are monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation, action or sanction.
- That monitoring of software/systems are implemented and updated as agreed in 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/Agreement (specifies details about acceptable contact) (AUP)
- They report any suspected misuse or problem to the Headteacher/Online safety Subject Leader for investigation, action or sanction.

- All digital communication with pupils/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.

Child Protection/Safeguarding Designated Person:

Is trained in online safety issues and is 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 and potential or actual incidents of grooming.
- Cyber-bullying

Pupils:

- Are responsible for using the school digital technology systems in accordance with the **online code of conduct which was devised by the pupils themselves.**
- 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 taking/use of images 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.

Parent/Carers:

Parent/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand the issues through parents evening, newsletters, letters, website and information about national/local online safety campaigns/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.
- Use of twitter.
- Access to parents' sections of the website

Community Users:

Community users who access school systems/website 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

As advised in "Teaching Online Safety in School," (DFE, June 2019) we adopt a whole school approach to the teaching of online safety that goes beyond teaching to include all aspects of school life, including culture, ethos, environment and partnerships with families and the community.

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 the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

content: being exposed to illegal, inappropriate or harmful material;
 contact: being subjected to harmful online interaction with other users; and
 conduct: personal online behaviour that increases the likelihood of, or causes, harm.
 commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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

- A planned online safety curriculum is provided as part of computing/PHSE/other lessons and is regularly revisited.
- School Digital Leaders are appointed to reinforce online safety advice across school.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

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

Education – Parents/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/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, parent/carer information boards and school web site.
- Parent/carers evenings/sessions.
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications eg.
www.swgf.org.uk
www.safeinternet.org.uk
<http://http://www.childnet.com/parents-and-carers>
www.thinkyouknow.co.uk (CEOP)

Education –The Wider Community

The school will provide opportunities for local community groups/members of the community 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 messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community and to help support community groups e.g. Early Years settings, Childminders, voluntary groups to enhance their online safety provision.

Education and 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:

- An audit of online safety training needs of all staff will be carried out regularly.
- All new staff should 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 Subject Leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The online safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online safety Subject Leader will provide advice/guidance/training to individuals as required.

Training - Governors:

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of the standards committee. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or any other relevant organisation.
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies, lessons or workshops).

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network 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.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Agilisys 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.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by St Helens. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtered changes.
- The school has provided enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record activity of users on the school technical systems and users are made aware of this in the Acceptable User Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person. (Agilisys)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date 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 system.
- An agreed policy is in place regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital images 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, parent/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 but 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 is not covered by the Data Protection Act) To respect everyone's privacy and in some cases protection, 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 school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website or school social media accounts will be carefully selected and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, blog or social media, particularly in association with photographs..
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (covered as part of an agreement signed by parents or carers at the start of the year)
- Pupils work can only be published with the permission of the pupil and parents or careers.

Data Protection

GDPR provides 8 main rights for individuals and strengthens those that already exist under the current Data Protection Act 1998.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making and profiling

Personal data will be recorded, processed, transferred and made available according to GDPR 2018 which states that personal data must be:

- Accessed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purpose it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing'
- It has a Data Protection Policy
- It appoints a Data Protection Officer
- It is registered as a Data Controller for the purposes of GDPR
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- A data protection impact assessment (DPIA) will:
 - be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy;
 - allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur;
 - be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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.
- The device must offer approved 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.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school e-mail 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 school e-mail service to communicate with others when in school, or on school systems (eg by remote access)
- 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 parents/carers (e-mail, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- 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 e-mail addresses, and twitter accounts should be used to identify members of staff.
- When sending emails to multiple recipients outside of the Council, e.g. parents, BCC must be used to avoid sharing of personal email addresses.

Social Media – Protecting Professional Identity

All schools, academies and local authorities have a duty 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, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information.

- Training to include: acceptable use, social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions, Risk assessment, including legal risk School staff should ensure that:
- Expectation of no engagement 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 schools use of social media for professional purposes will be checked regularly by the online safety Subject Leader.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use

Unsuitable/inappropriate activities

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

User Actions

		Acceptable	Acceptable at certain times	Acceptable Nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, data, transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) Contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using the school systems to run a business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X		
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial/personal information, database, computer/network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files.					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
On-line gaming (non-educational)				X		
On-line gaming (educational)				X		
On-line shopping/commerce				X		

File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting eg Youtube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need 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 (see User Actions above)

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or 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.

Other incidents

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

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

- Have more than one senior member of staff involved in the 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 pupils 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:
 1. Internal response or discipline procedures
 2. Involvement by Local Authority or national/local organisation (as relevant)
 3. Police involvement and/or action.
- If content being reviewed included images of child abuse then the monitoring should be halted and referred to the Police immediately. The computer in

question should be isolated immediately; any change to its state may hinder later Police investigation.

Other instances to report to the Police would include.

1. Incidents of 'grooming' behaviour
2. The sending of obscene materials to a child
3. Adult material which potentially breaches the Obscene Publication Act *Criminally racist materials
4. Other criminal conduct, activity or materials.

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Cyber-Bullying

We recognise that children's use of the internet may lead to incidents of cyber-bullying. Cyber-bullying is defined as the use of electronic communication to bully a person and can take many forms. While incidents of cyber-bullying are likely to occur out of school, pupils' online safety lessons are designed to warn them about cyber-bullying, promote respect online and inform them about how to respond to incidents of cyber-bullying. Should staff become aware of incidents of cyber-bullying between pupils, they should adopt a restorative solution approach as outlined in the anti-bullying policy. In addition to this, the parents/carers of the pupils involved will be given information and advice about how to monitor their children's internet use.

Child on child sexual violence and sexual harassment

Sexual violence and sexual harassment can occur between two children of any age and sex, including those of primary school age. They can occur online and face to face (both physically and verbally) and are never acceptable. All staff working with children are advised to maintain an attitude of '**it could happen here.**'. Any reported instances of child on child sexual violence or harassment must be reported to the DSL and dealt with in accordance with the safeguarding policy. Should any images be recorded on internet enabled devices, **staff should always avoid viewing them** as to do so would be a criminal offense.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. These include, but are not limited to; unauthorised access to school computers; or making, supplying or obtaining malware with the intent to damage the school network.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the **Cyber Choices** programme. This is a nationwide

police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

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 an appropriate 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.

Other related policies and relevant documentation

Social media policy

Employee code of conduct

Keeping Children Safe in Education

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

[Working together to safeguard children - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

[Stat guidance template \(publishing.service.gov.uk\)](http://publishing.service.gov.uk) (What to do if you're worried a child is being abused).

[Sexual violence and sexual harassment between children in schools and colleges - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

