Online SafetyPolicy

Approved by:	**Governing body – Helen Thompson**	
Last reviewed:	**September 2023**	
Next review:	**September 2025**	

Contents

Development/Monitoring/Review of Policy 3
Scope of the Policy 4
Legislation and Guidance 5
Roles and Responsibilities 5
Policy Statements 11
Education – Pupils 13
Education – Parents/Carers.....13
Education & Training - Staff & Volunteers.....13
Training -Governors.....14
Cyber-bullying 14
Acceptable use of the internet in school 15
Staff using work devices outside of school 16
Pupils using mobile devices in school 17
Mobile Technologies 17
Technical Infrastructure/ equipment, filtering and monitoring.....18
Use of digital and video images 19
Data Protection.....21
Communications 23
Social media 25
Unsuitable inappropriate activities 27
Response to misuse 29
Other incidents 31
School Actions and Sanctions 33
Other Policies 36

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Computing Lead
- Staff – Technical staff, DSL
- Governors
- Head Boy/ Head Girl on behalf of the children
- Local PCSO

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

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety policy will bemonitored by the:	- *Head teacher* - *Computing Lead* - *DSL* - *Technician* - *Governors*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Bi-annually*
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:	*September 24*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA* *Safeguarding officer* *LADO* *Police* *Prevent*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering.
- Internal monitoring data for network activity
- School's data analysis
- Surveys/questionnaires of
    - pupils
    - parents / carers
    - staff

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 students / 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 of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (seepolicy). 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.

Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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
- Relationships education
- 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 the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving 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:

- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting
- ensure that all staff undergo relevant training and staff understand their expectations, role and responsibilities around filtering and monitoring
- ensure staff receive regular online safety updates so that they are continually provided with the relevant skills and knowledge to effectively safeguard children

- ensure children are taught how to keep themselves and others safe online
- ensure, where necessary, that teaching that online safety is adapted for vulnerable children and those with special educational needs/disability

Headteacher /Senior Leaders:

- The Headteacher is responsible for ensuring that staff understand the policy and that it is being implemented consistently throughout the school.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management 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 dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Lancashire Authority disciplinary procedures).
- The Headteacher /Senior Leaders are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their online safety roles.
- The Headteacher /Senior Leaders will ensure that there is a system in place to allow for 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. Termly meetings (at least) will be held to look at procedures, incidents, monitoring reports etc

Computing Lead:

- attends the termly meetings to discuss current issues, review incident logs and filtering / change control logs
- takes day to day responsibility for online safety issues (alongside the safeguarding team) 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 (alongside the safeguarding team)
- liaises with school technical staff
- receives reports of online safety incidents (via CPOMS) and uses these to inform future online safety developments
- reports to the relevant meeting of Governors

Technical staff:

Technical Staff is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority 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
- putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. (see *Technical Security Policy*)
- 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 is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- conducting a full security check and monitoring the school's ICT systems on a twice-termly basis

All Staff and Volunteers

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 maintain an understanding of this policy
- they implement this policy consistently
- they know that the DSL is responsible for the filtering and monitoring systems and processes, and are aware of how to report any incidents of those systems or processes failing
- they follow the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- they work with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- they respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- they have read, understood and signed the *Staff Acceptable Use form*
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications 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 Policy 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
- Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read

and follow it. If appropriate, they will be expected to agree to the terms on acceptable use

Designated Safeguarding Lead

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Liaising with the Lancashire Authority
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the DSL with:

- the production / review / monitoring of the school Online Safety Policy.
- the production / review / 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 / incident logs
- consulting stakeholders – including parents / carers and the pupils about theonline safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- are responsible for using technology sensibly and appropriately
- have a good understanding of research skills and the need to avoid plagiarismand 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 devicesand digital cameras. They should also know and understand policies on the taking
  / 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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, 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
- their children's personal devices in the school
- good practise when using the internet at home

Policy Statements

Education – Pupils

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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.

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 / 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 / content they access on-line 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes arein place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – 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.

Parents/Carers are expected to notify a member of staff or the headteacher of any concerns or queries regarding this policy

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

- Curriculum activities
- Letters, newsletters, website, school's Facebook page
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

The school website will provide online safety information for the wider community

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. 'In order for schools and childcare providers to fulfil the Prevent duty, it is essential that staff are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified,' (DfE2015, The Prevent Duty)

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.

- 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 Agreement.
- The Computing Lead 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 / team meetings / INSET days.
- The DSLs and Computing Lead will provide advice / guidance / training to individuals as required.
- Regular Child Protection updates for all staff with reference to radicalisation and extremism as necessary.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee involved in technology, online safety, health and safety or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been

spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examine Devices

The headteacher, and any member of staff authorised to do so can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Artificial Intelligence

- Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
- Peel Park recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.
- Peel Park will treat any use of AI to bully pupils in line with our behaviour policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Acceptable Use of The Internet in School

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

Staff Using Work Devices Outside of 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 by always installing the latest updates

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

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

Pupils Using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them during lessons, clubs or play/dinner times. They must be switched off and in bags during the school day.

Any pupils seen using their phones during the school day will result in the confiscation of their device.

Mobile Technologies (including bringing own devices)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the *Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage*. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school Acceptable Use Agreements for staff, pupils and parents/carers gives consideration to the use of mobile technologies.

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 school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- Children across the school will access the computers and laptops using class logindetails.
- All KS2 users will be provided with a username and password by the schools ICT technician for access to websites such as, Ed Shed and TT Rockstars. The technician will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. On request, these passwords will be reset to ensure they remain secure.
- EYFS and KS1 pupils will use class generic login details to access the network. They will be gradually introduced to individual passwords to access websites and apps that we have subscribed to as a school with Individual passwords to access the network will be gradually introduced in KS2.
- The “administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- The ICT technician is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number

of licenses purchased against the number of software installations.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updatedand internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist andextremist material when accessing the internet in line with the Counter Terrorism and Securities Act 2015.
- The school has provided differentiated user-level filtering. Access is differentiated for staff and this is allocated when appointed and after the 'User Account Authorisation form' has been completed and approved by the schools SLT. The children filtering level is not differentiated and is all filtered using **Surf Protect.**
- The school uses **Securus 360** to accurately monitor digital users in line with KCSIE.
- School 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.
- 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" (eg trainee teachers, supply teachers, visitors and parents) onto the school systems. A 'guest' account is available for a visitor that ensures they can't access the Teachers or photo drive. Supply teachers or trainee teachers who may need access will complete a *User Account Authorisation form* before an account is created and access is granted. Parents who need access to computers will also sign in as a guest and during the 'housekeeping' acceptable use will be discussed. In addition, everyone who logs on to the system as a 'guest' will need to read the agreement on the desktop and click to confirm that they agree to this.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices. The schools IT technician is responsible for this and requests should be made to him when appropriate.
- An agreed policy is in place regarding the use of removable media (eg 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. (see *School Personal Data Policy*)

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 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 about therisks 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.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- 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 / 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. 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.

- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on the website or social media sites, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents orcarers.

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.

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 purposes 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". (see Privacy Notice)
- It has a *Data Protection Policy*
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs). These are the Head Teacher and the schools bursar.
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transferof personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data. This is recorded within the Safeguarding policies.
- There is a policy for reporting, logging, managing and recovering from information risk incidents. This can be found within the *Data protection policy (linked to the GDPR).* A disaster recover folder is also available via the schools technician.
- There are clear Data Protection clauses in all contracts where personal data maybe passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office. (See the cloud policy).

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, onceit has been transferred or its use is complete

The *Personal Data Handling Policy*, provides more information on the school's

responsibilities and good practice.

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 the 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 e.g. tablets, gaming devices	/							/
Use of personal email addresses in school, or onschool / academy network				/				/
Use of school / academy 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 *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are 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 (email, social media, chat, blogs, VLE etc) must be professional in tone and content.

Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class / group email addresses may be used at with KS1 and KS2, they will be provided with a school 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.

Social Media - Protecting Professional Identity

All schools, academies 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, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable tothe 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:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking ofsettings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal

riskSchool 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 membersof 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 social media accounts have been established following:

- A process for approval by senior leaders
- A development of clear processes for the administration and monitoring of these accounts – involving at least two members of staff. This being the Deputy Head teacher, office admin and schools ICT technician.
- A code of behaviour for users of the accounts, including
  - Systems for reporting and dealing with abuse and misuse
  - Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. Inall cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to report on despicable postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Unsuitable / 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 / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data	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 actsagainst 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 violenceor mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network accesscodes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others intheir use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)				X		
On-line gambling				X		
On-line shopping / commerce			X			
File sharing		X				
Use of social media			X			
Use of messaging apps		X				
Use of video broadcasting e.g. Youtube		X				

Actions will be carried out in accordance to the *Electronic devices, search and deletion policy*, if necessary.

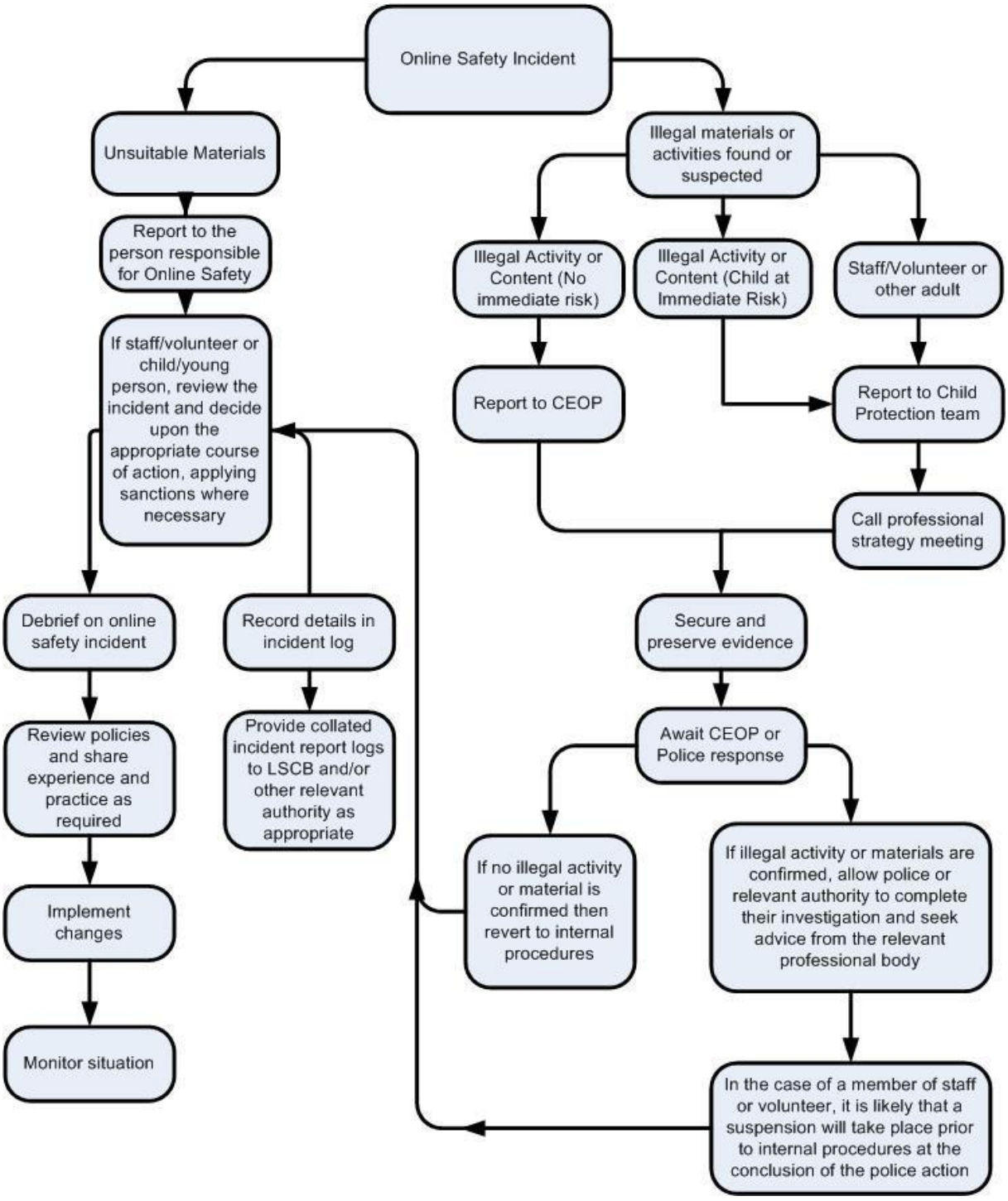
Response To Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Illegal Incidents

If there is any suspicion that the web site(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.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

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

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

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

- **If content being reviewed includes images of Child abuse then the monitoring shouldbe halted and referred to the Police immediately. Other instances to report to thepolice wouldinclude:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- **Isolate the computer in question 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with 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:

	Actions / Sanctions								
Pupils Incidents	Refer to class teacher	Refer to DSL	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites duringlessons	X								
Unauthorised / inappropriate use of mobile phone /digital camera / other mobile device	X								
Unauthorised / inappropriate use of social media /	X	X			X	X			

messaging apps / personal email									
Unauthorised downloading or uploading of files	X	X	X		X	X			
Allowing others to access school network bysharing username and passwords	X	X	X		X	X			
Attempting to access or accessing the school network, using another pupil's account	X								
Corrupting or destroying the data of other users	X	X			X				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X			X
Continued infringements of the above, followingprevious warnings or sanctions	X	X	X			X			
Actions which could bring the school into disreputeor breach the integrity of the ethos of the school	X	X	X			X			X
Using proxy sites or other means to subvert the school's filtering system	X	X	X	X	X	X	X	X	X
Accidentally accessing offensive or pornographicmaterial and failing to report the incident	X				X				
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		X

Staff Incidents	Actions / Sanctions							
	Refer to line manager	Refer to Headteacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access materialthat could be considered illegal (see list in earliersection on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X				X		X
Unauthorised downloading or uploading of files		X		?	X			
Allowing others to access school network by sharingusername and passwords or attempting to access or accessing the school network, using another person'saccount		X			X			X
Careless use of personal data e.g. holding or transferring data in an insecure manner		X			X	X		
Deliberate actions to breach data protection or network security rules		X		?	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		?				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digitalcommunications with students / pupils		X			X	X	?	X

Actions which could compromise the staff member'sprofessional standing		X				X		?
Actions which could bring the school into disrepute orbreach the integrity of the ethos of the school		X				X		?
Using proxy sites or other means to subvert the school's filtering system		X			X	X		?
Accidentally accessing offensive or pornographicmaterial and failing to report the incident		X			X	X		?
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X			X	X		
Continued infringements of the above, following previouswarnings or sanctions		X						X

These actions/sanctions have been discussed and agreed at the Online Safety workinggroup. Those that have been identified as a question mark will be decided upon the severity of the incident.

Other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy