Approved by: Pat Kerton Chair of Governors		**Date:** November 2022
Last reviewed on:	November 2022	
Next review due by:	November 2023	

Online Safety Policy

Development/Monitoring/Review of this Policy

This online safety policy has been developed through consultation with the whole school community through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Governing board:	*Yearly*
The implementation of this online safety policy will be monitored by the:	*The Digital Learning Group & the Senior Leadership Team*
Monitoring will take place at regular intervals:	*Yearly*
The Governing board 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:	*Yearly*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA Safeguarding Officer, Barnardo's designated corporate safeguarding lead, Berkshire West LSCB, LADO, Police, CEOP*

The school will monitor the impact of the policy using:

- Logs of reported incidents
    - Behaviour and bullying events on Sleuth
    - Safeguarding incidents on CPOMS
- Monitoring logs of internet activity (including sites visited)/filtering
    - Firewall monitoring through smoothwall
- Surveys/questionnaires of
    - Young people
    - parents/carers
    - staff

Purpose

This policy applies to all staff, volunteers, parents/carers, visitors and young people who have access to and are users of school digital technology systems, both in and out High Close School. It is designed to keep all users safe while working online.

Our school aims to:

- Have robust processes in place to ensure the online safety of 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE) National Minimum Standards for the welfare of children, Residential special schools: national minimum standards, and statutory guidance, Keeping Children Safe in Education, and the advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department'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 that empowers Principals to such extent as is reasonable, to regulate the behaviour 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 online-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.

In addition to the Equality Act 2010, it also 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 electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account aspects of the National Curriculum computing programmes of study and the Education for a Connected World framework.

This policy complies with our funding agreement and articles of association.

The procedure in which online safety incidents are dealt with is outlined in this policy but will also be in line with the following High Close School Policies.

- Promoting Positive Behaviour and Relationships
- Countering Bullying
- Child Protection and Safeguarding
- Staff disciplinary, Grievance and Whistleblowing

And the following Barnardo's policies

- Data Protection Policy
- Barnardo's Safeguarding Policy
- IT Code of Conduct

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.

The governing board has overall responsibility for monitoring this policy and holding the principal to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Richard Woodley**.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school by

- Being aware of the procedure to be following in the event of serious allegation made against a member of staff alongside (at least) another member of the Senior Leadership Team.
- Providing training as required
- Allow for monitoring and support

Designated Safeguarding Leads & Digital Learning Officer

The DSLs will work with the DLO to take responsibility for online safety in school, in particular:

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the principal, network manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the principal and/or governing board
- Leading the Digital Learning Group when it comes to online safety
- Having a leading role in establishing and reviewing the school online safety policies / documents
- Should be trained and train other members of the school community in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

Digital Learning Group

Online Safety is one of the responsibilities of the Digital Learning Group as 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.
Members of the Digital Learning Group will assist the Digital Learning Officer with:

- The production/review/monitoring of the school online safety policy/documents.
- The production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- Mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- Monitoring network/internet/filtering/incident logs
- Consulting stakeholders – including parents/carers and the LA about the online safety provision
- Monitoring improvement actions identified through use of the 360 degree safe self-review tool

Network Manager

The Network Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep users safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring that servers, wireless systems and cabling must be securely located and physical access restricted
- Ensuring that all users may only access the school's networks through a username provided and a properly enforced password protection policy
- Ensuring that all users will have clearly defined access rights to school technical systems and devices.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 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
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring they follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Reporting any suspected misuse or problem to the relevant member of staff for investigation
- Embedding Online safety issues in all aspects of the curriculum and other school activities
- Monitoring ICT activity in lessons, extra-curricular and extended school activities
- In lessons where internet use is pre-planned, guiding young people 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

Parents / Carers

Parents / carers are expected to:

- Notify a member of staff or the principal of any concerns or queries regarding this policy
- Ensure their young person has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Seek advice on all areas of online safety including how to update privacy settings and monitor their children's interactions on social media.
- support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
    - digital and video images taken at school events
    - access to parents' sections of the website/Learning Platform and on-line pupil records
    - their children's personal devices in the school (where this is allowed)

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-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

Visitors and members of the community

Visitors and members of the community, including pupils, 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 relevant terms on acceptable use.

Education and Training

Young People

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum. The safe use of social media and the internet will therefore be covered in other subjects where relevant. The school will use assemblies and Internet Safety day to raise awareness of the dangers that can be encountered online and may also invite speakers to talk to young people about this.

Learning about online safety takes place in several different formats around the school. In addition to formal lesson time designated in the school timetable, focus is given to online safety in unit areas and specific keyworking is completed with individuals around staying safe online. These sessions are recorded in the keyworking files. The Family Resource Team also target groups of young people who need further intervention and education around online safety. Both care and education staff focus on the objectives listed below for the different age groups.

Pupils work towards independence while at school, progress for which is recorded on the Pupil Independence Grid (PIG)

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 internet searches being blocked. In such a situation, staff can request that the Network Manager 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.

To ensure it meets the learning objectives listed, the content of the curriculum will refer to DfE Teaching Online Safety in Schools, Education for a Connected Word Framework and SWGfL Project Evolve – online safety curriculum programme and resources among many other resources to meet the following learning objectives:

in **Key Stage 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
- 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

in **Key Stage 3**, will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

in **Key Stage 4** will be taught to:

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, they will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

Parents / Carers and The Wider Community

This policy will also be shared with parents / carers and will be made available on the school website. The school will also seek to provide information and awareness to parents and carers and the wider community through:

- Offering support through the family Resource Team support
- Maintaining strong contact with care and education staff
- Raising awareness during parents' evenings and other whole school events
- Providing family learning courses in use of new digital technologies, digital literacy and online safety onsite and online
- Targeted online safety messages via Parenthub / Twitter / Facebook
- Sharing online safety expertise/good practice with local schools and community groups
- Keeping the school website with up to date and relevant information

Parents / carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- National Crime Agency's CEOP Command education programme - ThinkuKnow

If parents / carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their Young Person's key/link worker

Concerns or queries about this policy can be raised with any member of staff or the Principal.

All staff and 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:

- All new staff will complete the Thinkuknow Introduction Course in their first year of employment and every other year after that
- Staff that have completed the Thinkuknow Introduction Course will be offered to complete additional units
- Thinkuknow Factsheets for Professionals will be made available to all members of staff

Acceptable use policy

Acceptable use of the internet in school

All young people, parents, 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 young people, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

The acceptable use of internet in school would include cases where staff and pupils have been granted access to the school network on their own devices.

Use of mobile devices in school

Mobile devices may be brought in by young people but must adhere to the school rules regarding their use, even if they are not using the school network to access the internet but 3G, 4G or 5G instead.

Most young people will not be allowed to have their devices with them on site and those who have been allowed to, for a very specific set of reasons, must not use their mobile phones within lessons, and staff have the right to confiscate mobile phones if they are being used inappropriately.

If there are concerns about content on their mobile devices, then staff may confiscate these devices so the concerns can be investigated by the appropriate people. Parents and carers will be informed of any such concerns.

Any use of mobile devices in school by young people must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a young person may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff should follow the guidance within the Staff Code of Conduct regarding mobile devices.

Use of digital and video images

- 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 young people about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Written permission from parents or carers will be obtained before photographs of young people are published on the school website/social media/local press (covered as part of the AUA signed by parents or carers at the start of the year)
- 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, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other young people 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 young people are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images.
- A young person's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Young person's work can only be published with the permission of the young person and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school must ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school may also have appointed a Data Manager and Systems Controllers to support the DPO
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only 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. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected. (be sure to select devices that can be protected in this way)
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

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:

	Staff & other adults				Young People			
Communication Technologies	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	X				X			
Use of mobile phones in lessons (exceptional circumstances / emergency)			X				X	
Use of mobile phones in social time		X				X		
Taking photos on personal mobile phones/cameras				X				X
Taking photos on school mobile phones/cameras	X						X	
Use of other mobile devices e.g. tablets, gaming devices	X					X		
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails (e.g. pupil communication with carer)				X		X		
Use of messaging apps		X				X		
Use of social media		X				X		
Use of blogs		X				X		

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. Staff and should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. 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 young people or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- KS2 will be provided access to an email platform while KS3 and above will be provided with individual school email addresses for educational use.
- 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

We have a duty of care to provide a safe learning environment for young people and staff. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school 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 young people, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: 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:

- No reference should be made in social media to young people, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

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

Personal Use:

- Personal communications are those made via a personal social media account. In all 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 pro-actively monitor the Internet for public 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 governor that overseas online safety and Digital Learning Group to ensure compliance with the school policies.

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.

The response to cyber-bullying incidents will be in line with the school Countering Bullying Policy.

Dealing with 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 users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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	
	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						X

• Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping/commerce		X	X		
File sharing	X				
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting (Limited to Microsoft 365 Stream)		X			

Responding to incidents of misuse

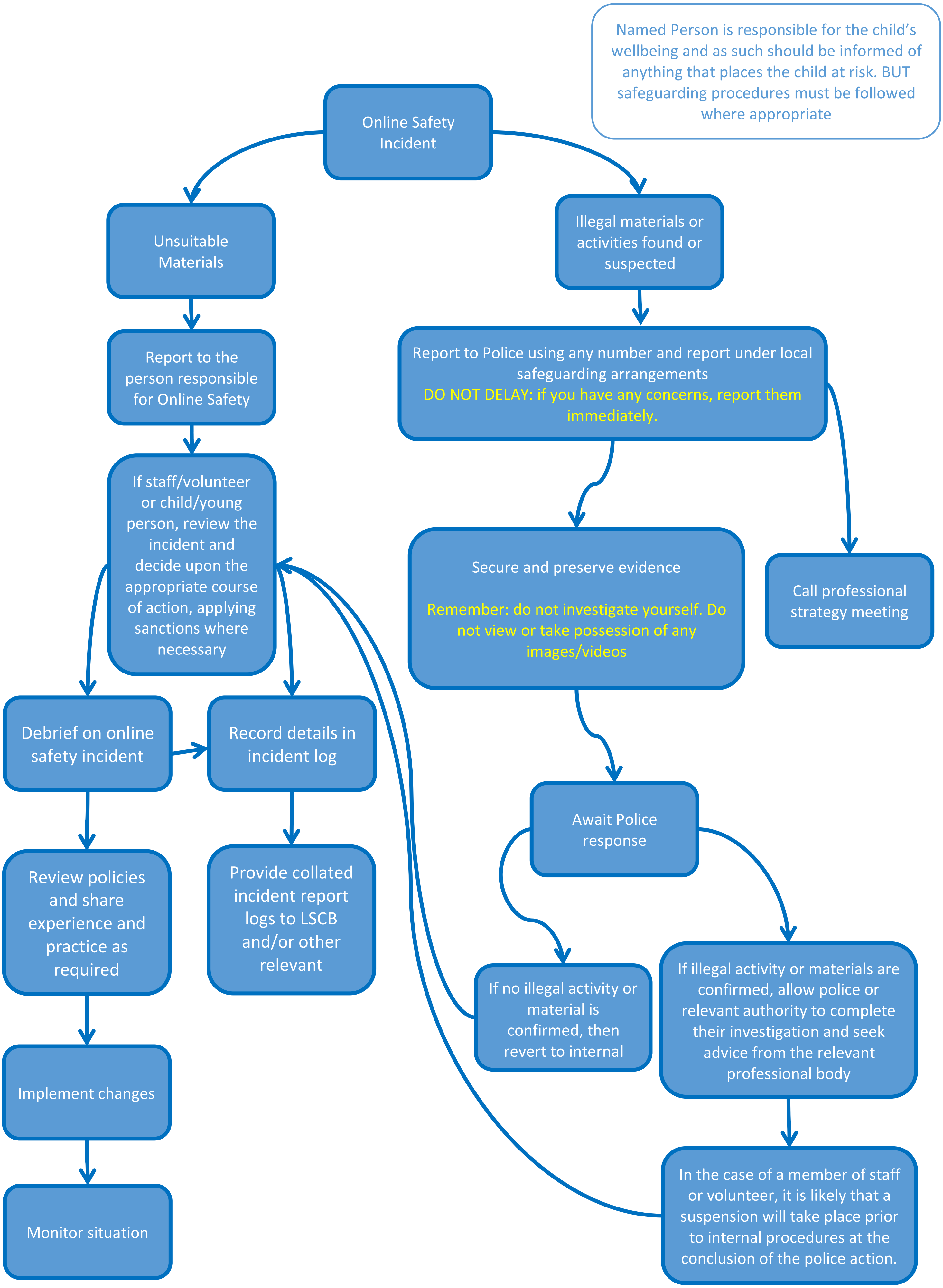
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If you find inappropriate or illegal material on a PC or other electronic device, do not send it to anyone to report it as this can be classed as distributing illegal or offensive material.

The flowchart on the next page is expected to be followed for any incidents around Online safety.

Staff must refer any Safeguarding concerns to the Designated Safeguarding Leads in the first instance if the concerns are about a young person.

If the incident involves staff then disciplinary procedures would be followed as outlined in Staff disciplinary, Grievance and Whistleblowing. If the incident involves a young person then procedures will be followed detailed in Promoting positive behaviour and relationships (Discipline including sanctions, rewards and restraints) and dealt with on an individual basis dependent on the young person and their needs. Incidents of online bullying will be dealt with in accordance to the schools Countering Bullying policy.



Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate

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

Record details in incident log

Review policies and share experience and practice as required

Provide collated incident report logs to LSCB and/or other relevant

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements
DO NOT DELAY: if you have any concerns, report them immediately.

Secure and preserve evidence

Remember: do not investigate yourself. Do not view or take possession of any images/videos

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal

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.

Recording of other incidents

All Online safety incidents concerning young people will always be recorded and documented following the same agreed procedures as other types of incidents.

Online safety incidents concerning staff should be recorded through supervision notes, as any other incident would be recorded.

The school's Network Manager will inform the designated safeguarding leads of any inappropriate searches flagged up through the filtering system that come under possible safeguarding.

DSLs will report any incident that falls under the under the Counter-Terrorism and Security act 2015 to prevent people being drawn into terrorism by reporting any concerns of extremism to the Prevent Officer at Thames Valley Police.

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								
Incidents	Refer to class teacher/tutor	Refer to Head of	Refer to Headteacher/Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access	Warning	Further sanction e.g.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X	X	X	X		
Unauthorised use of non-educational sites during lessons	X				X			X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X					X		X	
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X				X		X	
Unauthorised downloading or uploading of files	X	X			X	X	X		
Allowing others to access school network by sharing username and passwords	X				X		X		

Attempting to access or accessing the school network, using another pupil’s account	X	X			X		X		
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X		
Corrupting or destroying the data of other users	X	X	X		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, following previous warnings or sanctions	X	X			X		X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X		X	X		X	
Using proxy sites or other means to subvert the school’s filtering system	X	X			X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X						X	
Deliberately accessing or trying to access offensive or pornographic material	X	X			X	X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X			X	X	X		

	Actions/Sanctions							
Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X	X			
Inappropriate personal use of the internet/social media/personal email	X							
Unauthorised downloading or uploading of files	X							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules	X				X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				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 digital communications with	X	X	X			X		X
Actions which could compromise the staff member's professional standing	X	X	X			X		X
Actions which could bring the school into disrepute or 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		
Accidentally accessing offensive or pornographic material and failing to report the incident	X					X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	

Breaching copyright or licensing regulations	X				X	X		
Continued infringements of the above, following previous warnings or sanctions	X	X			X		X	

Acceptable Use agreements

Staff and young people are expected to abide by the Acceptable Use agreements. These have been modified for the young people in primary and in secondary from standard Acceptable Use Agreements to take into account the young people’s Special Educational Needs. Parents and carers will also be expected to sign the Parent and Carer’s agreement that they will support the school’s policy regarding Online Safety.