Basnett Street Nursery School
& The Chatterbox Club

Online Safety Policy

2024-2026

This policy has been reviewed by:

- **Headteacher – Mrs Lindsay Ingham**
- **Online Safety Officer Coordinator – Carol Carpenter**
- **Lead Teacher – Miss Emma Barker**
- **Governors - Safeguarding Governor – Mrs Thelma Cullen**
- **Governor – Online Safety - Mrs Helen Mansfield**

Schedule for Review

This online policy was approved by the *Board of Directors* / Full *Governing Body / Governors Sub Committee on:*	Full Governing Body Meeting 13/12/2023
The implementation of this online policy will be monitored by the:	Headteacher
Monitoring will take place at regular intervals:	Annually reviewed
The *Governing Body* will receive a report on the implementation of the online policy generated by the monitoring group (which will include anonymous details of online incidents) at regular intervals:	Every term
The Online Safety Policy will be reviewed bi-annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online or incidents that have taken place. The next anticipated review date will be:	December 2026
Should serious online incidents take place, the following external persons / agencies should be informed:	Lindsay Ingham, Emma Barker, Carol Carpenter and Grace Walker

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering and monitoring logs of internet activity
- Internal monitoring of network activity
- Staffsafe / CPOMS to log any incidents
- Acceptable use policy for staff
- Advice to parents on safer internet use
- Parent surveys

Introduction

This policy applies to all members of the school community (including staff, children, parents/carers, visitors and school community users). Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

The School's Vision for Online

Basnett Street Nursery School and The Chatterbox Club provides a diverse, balanced and relevant approach to the use of technology. All children will be encouraged to maximise the benefits and opportunities that technology has to offer Children learn in an environment where security measures are balanced appropriately and responsibly. The school recognises the risks associated with technology and how to deal with them, both within and outside the school environment. All users in the school community understand the need for an Online Safety Policy.

Scope of the Policy

This policy applies to all members of the *school* community (including staff, children, 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 children 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 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Policies and Practices

Children have access to the internet in the nursery environment, by the internet filtering Securly Software which is a centrally hosted web filtering provision enabling safe internet access to the school provided by The IT Dept. Securly provides daily reports and access to live monitoring. Children and staff use cameras and video cameras to support teaching and learning. Permission is sought from parents for us to use photos as part of our assessments and to display these on our school website and school Facebook page, school brochure and on school displays.

Mobile phone use is prohibited in the nursery, except on designated breaks. Facebook is used as a form of media to engage and communicate with our parents. We have opted to use a system and service that offers additional safety advice and measures.

In the event of an Online incident, staff should report the incident to Carol Carpenter and Lindsay Ingham / Emma Barker.

This Online policy should be read in conjunction with the following other related policies and documents:

- Safeguarding & Child Protection Policy
- Handling Allegations of Abuse against Staff
- Handling Concerns about the Welfare and Safety of children and Young People
- Health and Safety
- Mobile phone and social networking
- ICT Acceptable Use Policy
- Social Media & Networking Policy

Roles and Responsibilities

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

- **Headteacher – Mrs Lindsay Ingham**
- **Online Safety Officer Coordinator – Mrs Carol Carpenter**

- **Staff – Lead Teacher – Miss Emma Barker**
- **Governor – Safeguarding and Online Safety – Mrs Thelma Cullen**

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

- regular meetings with the Online Safety Coordinator
- regular monitoring of online incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Headteacher and Senior Leaders:

- The *Headteacher* has a duty of care for ensuring the safety (including online) of members of the school community, though the day to day responsibility for online will be delegated to the *Online Safety Coordinator*.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff. (see flow chart on dealing with online incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures).
- *The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online roles and to train other colleagues, as relevant.*
- 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 monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

Online Safety Coordinator:

The role of the Online Safety Coordinator in our school includes:

- Ensure operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- To ensure the policy is implemented and actively monitored.
- To ensure high levels of data protection, e.g. permission sought regarding the use of photos, information provided on the school's website and Facebook page.
- To ensure Facebook security systems are working effectively.
- To ensure use of mobile phones is prohibited in the nursery by parents and visitors.
- Ensure all staff are aware of reporting procedures and requirements should an online query or incident occurs.
- Ensure the Headteacher, SLT, staff, governors are updated as necessary.
- To liaise closely with the Headteacher to ensure a co-ordinated approach across relevant safeguarding areas.
- Provide safety advice/training for staff, parents/carers and governors.
- Ensure a safety Incident log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with safety issues through advice given by safeguarding agencies.

- takes day to day responsibility for online issues and has a leading role in establishing and reviewing the school online policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority / relevant body.
- receives reports of online incidents and creates a log of incidents to inform future online developments.
- meets regularly with Online Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant meeting / committee of Governors.
- reports regularly to Senior Leadership Team.

Managed Network Provider:

The IT Dept 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 technical requirements and any Local Authority / other relevant body Online 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 via group policy on the server.
- the filtering policy , is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with online technical information in order to effectively carry out their online role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Online Safety Coordinator for investigation. This is presented via the Securly Software.
- that monitoring software / systems are implemented and updated as agreed in school policies
- Monitoring any radical or ideology engagement on staff work logins & email
- Reporting to the head teacher any security breaches or virus risks
- Regular Reporting of Suspicious incidents emailed to the Headteacher

Teaching and Support Staff

Are responsible for ensuring that:

- They follow the school code of conduct.
- they have an up to date awareness of online matters and of the current *school* online policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) and Socail Media & Networking Policy
- they report any suspected misuse or problem to the *Headteacher, Senior Leaders ; Online Safety Coordinator* for investigation.
- all digital communications with pupils / parents / carers should be on a professional level
- online issues are embedded in all aspects of the curriculum and other activities
- children understand and follow the online and acceptable use policies
- children 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 children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection / Safeguarding Designated Person

Should be trained in online issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Children:

At Basnett Street Nursery School the children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond.

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 / VLE and information about national/ local online campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good online 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 / VLE and on-line pupil records

Community Use

The community play a crucial role in the use of internet/mobile devices in an appropriate way e.g. Parent Courses etc.

Policy Statements

Education – Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating *children* to take a responsible approach. The education of *children* in online is therefore an essential part of the school's online provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

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

- A planned online curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online messages should be reinforced as part of a planned programme of group time and activities
- Children 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.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children 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
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children 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, children 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 IT Department technicians 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 risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- *Curriculum activities*
- *Letters, newsletters, web site, VLE*
- *Parent /Carers evenings/sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g.* www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

- *Online messages targeted towards parents/Carers.*
- *The school website will provide online information for the wider community*

Education & Training – Staff / Volunteers

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

- A planned programme of formal online training will be made available to staff. This will be regularly updated and reinforced. An audit of the online training needs of all staff will be carried out regularly.
- All new staff should receive online training as part of their induction programme, ensuring that they fully understand the school online policy and Acceptable Use Agreements.
- *The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The Online Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.*

Training – Governors

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

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

Technical – Infrastructure, Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure / network is 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 responsibilities:

- School technical systems will be managed by The IT Dept who will ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy 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 / academy technical systems and devices.
- All users will be provided with a username and secure password by the online Safety Coordinator. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* or Online Safety Coordinator and kept in a secure place (e.g. school safe)
- is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. This is achieved through regular MS Office Reports.
- 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 updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- *The school has provided enhanced / differentiated user-level filtering. Currently levels are Staff / Student / Guest*
- *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.*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). All staff will report any issues to the Headteacher*
- Appropriate security measures are in place by LCC Education Digital Services who 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.
- All visitors will read and sign the AUP before use.
- *Staff can download education apps onto tablets or programmes to support teaching and learning. No staff members are allowed to use school devices that have been taken home for work purposes.*
- *Appropriate security measures are in place rregarding 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.

Communication Technologies

Basnett Street Nursery uses a variety of communication technologies and are aware of the benefits and associated risks. All new technologies are risk assessed before being employed throughout the school. The following are used technologies used within the school:

Email:

In our school the following statements reflect our practice in the use of email.

- All staff to use own email and computer logins and not a generic one excluding bursar@ and head@ email addresses.
- All staff uses the Microsoft Office 365 email system for emailing.
- Only official email addresses should be used to communicate with parents and other professionals.
- All staff are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), understanding that safe practice should be followed in respect of record keeping and security.
- All users of email are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- All users are aware they should not open attachments that they suspect may contain illegal content.
- Emails that look suspicious must be deleted immediately and reported to The IT Dept.

Social Media Networks:

In our school the following statements outline what we consider to be safe, acceptable and unacceptable use of Social Network sites:

- The system and service chosen by the school offers additional safety advice and measures.
- No personal details of children and staff will be given on Facebook.
- Comments will be monitored closely.
- To publish photographs and avoid them being tagged, a separate photo gallery facility is provided which is not run by Facebook. Viewers are prevented from posting comments below photographs of school activity and therefore, from identifying children indirectly, which would undermine our school policy.
- Images are made more difficult to access with this system because the usual ability to 'right click' and 'save as' has been disabled.
- The school provides a media area on the Facebook page that contains online videos and offers support to parents.
- The Facebook wall will be monitored by the school for interaction. Communications regarding individual children will never take place in this form.
- Staff will not befriend parents on Facebook unless pre-agreed with the Headteacher (for example pre-existing friendships)
- Children will not be added 'as friends' on Facebook.
- The Facebook wall is configured to not allow postings of photographs or videos by parents.
- The Facebook wall also has a profanity filter set to 'high' in place. This is a precautionary measure only in the unlikely event of inappropriate content being posted.
- Only audio recording (if appropriate), not videos, will be published via Facebook, to open up the learning environment to parents, without exposing the children to risk

Mobile Telephone:

- Staff, parents and visitors are not allowed to use mobile phones in school time.
- If a phone call needed to be made by a visitor, e.g. contractor, property group staff, then the call must be made in the parent's room away from the children.
- Staff can only use their mobile phones on designated breaks.
- School does not have a mobile phone; however, due to the number of children and staff, staff will carry their personal mobile phone in order to communicate with each other throughout the trip. No personal calls will be answered or made throughout the trip. Parent helpers will be informed that mobile phones must not be used, except for emergencies.
- Personal mobile phones of the office staff may be used in an emergency evacuation to contact the emergency services.

Instant Messaging:
Instant messaging is not used at Basnett Street Nursery School.

Virtual Learning Environment (VLE) / Learning Platform:
A Virtual Learning Environment is not available at Basnett Street Nursery School.

Web Sites and other Online Publications:
In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- All staff are aware that photos may only be published onto the website following permission sought from parents. No personal details will be attached to photos.
- The Business Manager updates the school website and ensures the content is relevant and current.
- The Headteacher, alongside the Business Manager, has overall responsibility for what appears on the website.
- The online policy will be accessible on the schools website
- All downloadable materials will be in a read-only format (PDF), to prevent content being manipulated and potentially re distributed without the schools' consent.

Video Conferencing:
In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- Permission letters will be made available for parents/carers to sign giving permission for their child/children to participate in video conferencing. It is important to note that children will not be appearing 'live' on the internet through a video conferencing link.
- Approval by the Headteacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/person(s) taking part.
- Pupils using video conferencing equipment will be supervised at all times.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

Others:
Basnett Street Nursery School will adapt / update our policy in light of emerging new technologies and any issues or risks associated with these technologies.

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:

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- The school seeks consent from parents/carers for the use of photos in the nursery environment, assessment files, school website, and Facebook page and school prospectus. This information is obtained at the beginning of the school year.
- Staff are aware that full names and personal details must not be used any digital media, particularly in association with photographs.
- All staff recognises and is aware of using personal social network sites. High professional conduct must be maintained at all times. Publishing images or comments in relation to work could lead to instant dismissal for any member of staff undertaking in such activity in relation to work.
- Staff understands that they must not store digital content on personal equipment, e.g. photos.
- Staff are aware photographs and videos should only be taken using school equipment and should only be used for school purposes and should only be made accessible to appropriate staff/pupils.
- When taking photos/videos, staff to ensure children are dressed appropriately and are not participating in activities that could be misinterpreted.
- All staff are aware of any children who photograph must not be taken for school purposes or external media.

Other Mobile Devices:

- As new technologies are introduced, their use is risk assessed and balanced against their potential benefits for learning.
- Devices are virus checked (if applicable) before use on school systems.
- All users are aware of the 'sanctions' for misuse of mobile devices.
- Device owners are aware that the school cannot be held liable for any damage or theft of personal devices.

Taking Photographs / Video:

- All staff are authorised to take photographs and video images.
- All photo and video cameras are school owned equipment. Personal equipment to store images are unacceptable and avoided.
- Staff ensures that photographs do not show children in any distress or misinterpretation and not continually favoured when taking images.

Parents Taking Photographs / Videos

- Under the Data Protection Act (1998) parents are entitled to take photographs of their own child and are reminded of this during school production etc.

Storage of Photographs / Video

- All photographs/videos are securely stored in the school environment.
- Images are not stored on staff personal equipment.
- No staff personal images are stored on school equipment.

- Staff ensure all photographs/video images are disposed/deleted once the image has lapsed.

Publication of Photographs / Videos

- Parental consent is always requested before the publication of any photographs or videos.
- Names and personal information are never accompanied with published images.

When Publishing Images

- All staff recognises and understands the risk associated with publishing images for the school.
- All staff ensure that personal profiles are secure and do not display content that is detrimental to their professional status of the school.

The Media, 3rd Parties & Copyright

- All media, 3rd parties and copyrights are supervised at all times and comply with the Data Protection requirements in taking, storage and transfer of images.

CCTV, Video Conferencing, VOIP & Webcams

- No CCTV Video conferencing or webcams are used in the school.
- See camera and recording device policy.

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

- 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".
- 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)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents

- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office. Ensure that M365/Sharepoint is used for this purpose.

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 (below) once it has been transferred or its use is complete.

Communications

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

	Staff & other Adults			
Communication Technologies	Allowed at certain times	Allowed for selected staff	Not Allowed	Allowed
Mobile phones may be brought to school	■			
Use of mobile phones in social time				■
Use of other mobile devices eg tablets, gaming devices		■		■
Use of personal email addresses in school, or on school network	■			

Use of school email for personal emails					
Use of messaging apps					
Use of social media					
Use of blogs					

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff or parents / carers (email, chat, 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.
- Children should be taught about online 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 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 to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

The *school's* use of social media for professional purposes will be checked regularly by the Headteacher and online coordinator to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

Examples of inappropriate incidents and how they will be dealt with are:

INCIDENT	PROCEDURE & SANCTIONS
Accidental access to inappropriate materials.	Minimise the webpage/turn the monitor off, inform Online Safety Coordinator who will enter details in the incident log and report to LGfL filtering services. Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	Inform SLT. Details will be entered in incident log. More serious or persistent offences may result in further disciplinary action. Record
Deliberate searching for inappropriate materials.	Inform SLT. Disciplinary action may be taken. Record
Bringing inappropriate electronic files from home.	Inform SLT. Remind of AUP. Disciplinary action may be taken. Record.
Using chats and forums in an inappropriate way.	Inform SLT. Disciplinary action will be taken.

The SLT and Online Safety Coordinator will be responsible for dealing with Online safety incidents. These will be monitored termly and more frequently as necessary and reported to governors.

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

User Actions		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	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

pass on, material, remarks, proposals or comments that contain or relate to:	**criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986**					X
	pornography					X
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using 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 (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line shopping / commerce (for school use)		x				
File sharing (for school use)		x				
Use of messaging apps					x	
Use of video broadcasting e.g. Youtube					x	

Responding to incidents of misuse

Incidents will be recorded in the incident log. This will be audited by the Online Safety Coordinator and SLT.

Any suspected illegal material or activity must be taken to the Headteacher who will refer this to external authorities, e.g. Police. The school will never investigate, interfere with or share evidence as this could be inadvertently being committing an illegal offence. Staff are aware that it is essential that correct procedures must be followed when preserving evidence to protect those investigating the incident. Potential illegal content will always be reported to the Internet Watch Foundation (http://www.iwf.org.uk). Staff must never try to investigate the incident themselves.

Examples of illegal offences are:

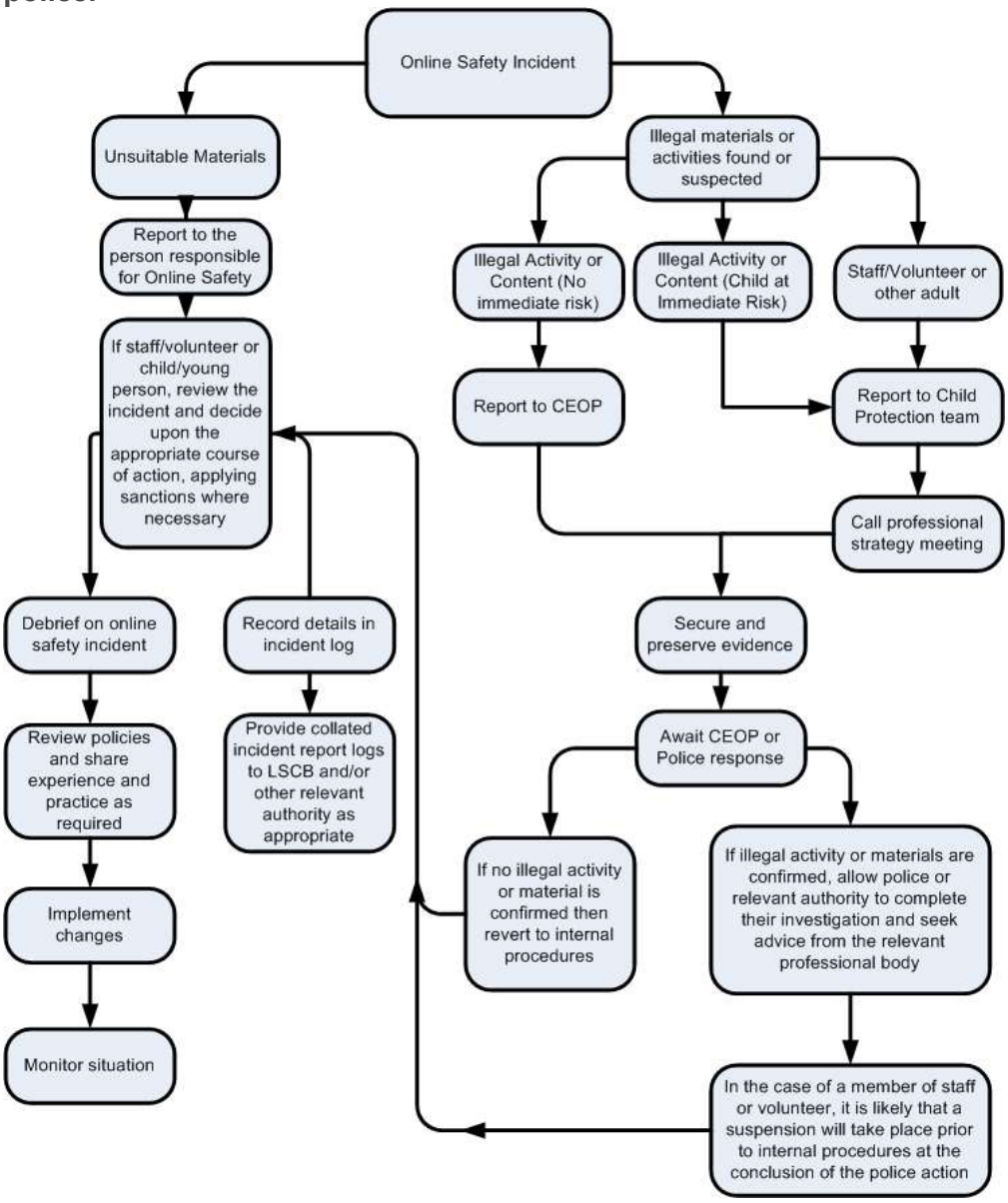
- Accessing child sexual abuse images.
- Accessing non-photographic child sexual abuse images.
- Accessing criminally obscene adult content.
- Incitement to racial hatred.

More details regarding these categories can be found on the IWF website.

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

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 and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

	Actions / Sanctions							
Staff Incidents	Refer to Line Managerr	Refer to Headteacher	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	X						
Unauthorised downloading or uploading of files	X	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				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			X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	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		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X				X		X
Actions which could compromise the staff member's professional standing	X		X			X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X						
Using proxy sites or other means to subvert the school's filtering system	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	
Breaching copyright or licensing regulations	X	X						X

Continued infringements of the above, following previous warnings or sanctions	X	X	X	X			X	X

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

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

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:

Evaluating the Impact of the Online Safety Policy

The Governing Body, Headteacher, Online Safety Champion have been involved in the writing of this policy and will monitor and evaluate the impact of safeguarding procedures throughout the school annually.

*****Appendices are filed in the Online Safety File – Main Office****