

# Basnett Street Nursery School



## Online Safety Policy

**2021-2022**

This online policy has been reviewed by:

- **Headteacher** – Mrs Lindsay Ingham
- **Online Safety Officer Coordinator** – Mrs Alison Boyd
- **Staff – Lead Teacher/ Online Governor** – Mrs Kim McGrail
- **Governors / Safeguarding Governor** – Mrs Thelma Cullen

•

Reviewed April 2021

---

## Schedule for Review

This online policy was approved by the <i>Board of Directors / Governing Body / Governors Sub Committee</i> on:	Summer Term 2021
The implementation of this online policy will be monitored by the:	Online Safety Coordinator
Monitoring will take place at regular intervals:	Annually reviewed
The <i>Governing Body</i> 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 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:	Every term
Should serious online incidents take place, the following external persons / agencies should be informed:	Alison Boyd, Lindsay Ingham, Kim McGrail and Grace Walker

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - parents/carers
  - staff

## 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 Schools 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 an internet filtering lightspeed system service which is a centrally hosted web filtering provision enabling safe internet access to the school provided by BT Lancashire Services. 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 Alison Boyd and Lindsay Ingham/Kim McGrail

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

- Safeguarding & Child Protection Policies
- 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
- 

## **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 Alison Boyd
- Staff – Lead Teacher/ Online Governor – Mrs Kim McGrail
- Governors / Safeguarding Governor – 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 school's Designated Senior Person 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
- liaises with school technical staff
- 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:**

BT Lancashire Services 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**
- the filtering policy (if it has one), 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 / Virtual Learning Environment / 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.
- that monitoring software / systems are implemented and updated as agreed in school policies

### **Teaching and Support Staff**

Are responsible for ensuring that:

- **they have an up to date awareness of online matters and of the current *school* online policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **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**

Reviewed May 2021

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 BT Lancashire Service 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](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://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

Reviewed May 2021

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 BT Lancashire Services 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 **Online Safety Coordinator** accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly 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.*
- *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 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 regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

### **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 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.
- All school emails include a standard disclaimer at the bottom of all out going email communications.

### **Social 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.
- 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.

### **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 school bursar updates the school website and ensures the content is relevant and current.
- The Headteacher, alongside the bursar, 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.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session, e.g. how to 'stop' or 'hang up' the call.
- 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.

Reviewed May 2021

- 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, 3<sup>rd</sup> Parties & Copyright**

- All media, 3<sup>rd</sup> 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
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- 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.

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

Reviewed May 2021

- 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:

Communication Technologies	Staff & other Adults			
	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
<b>Accidental access to inappropriate materials.</b>	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.
<b>Using other people's logins and passwords maliciously.</b>	Inform SLT. Details will be entered in incident log. More serious or persistent offences may result in further disciplinary action. Record

<b>Deliberate searching for inappropriate materials.</b>	Inform SLT. Disciplinary action may be taken. Record
<b>Bringing inappropriate electronic files from home.</b>	Inform SLT. Remind of AUP. Disciplinary action may be taken. Record.
<b>Using chats and forums in an inappropriate way.</b>	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:

<b>User Actions</b>		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					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography					X
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using 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	x				
File sharing	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:

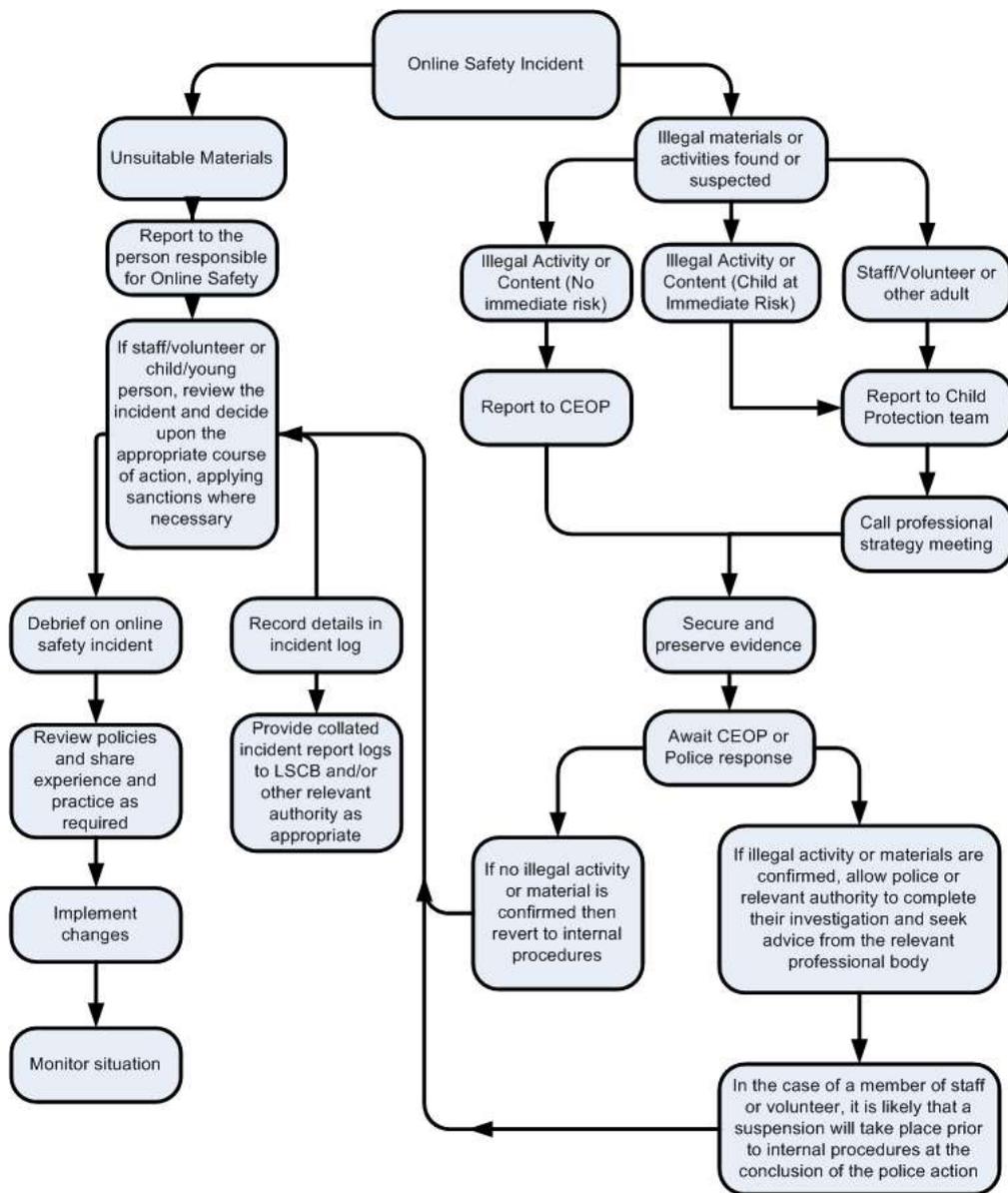
- Accessing child sexual abuse images.
- Accessing non-photographic child sexual abuse images.
- Accessing criminally obscene adult content.
- Incitement to racial hatred.

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:

Reviewed May 2021

- 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 Manager	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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		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

Acceptable Use Agreement

Use of Digital / Video Images

Staff (and Volunteer) Acceptable Use Policy Agreement

Acceptable Use Agreement for Community Users

Responding to incidents of misuse – flow chart

Record of reviewing devices / internet sites (responding to incidents of misuse)

Reporting Log

Training Needs Audit Log

School Technical Security Policy (including filtering and passwords)

School Personal Data Handling Policy

Appendix - DfE Guidance on the wording of the Privacy Notice

School Policy: Electronic Devices - Searching & Deletion

Policy Statements

Mobile Technologies Policy (inc. BYOD/BYOT)

Social Media

Legislation

Links to other Organisations or Documents

Glossary of Terms

### School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

#### **This Acceptable Use Agreement is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.



## Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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 pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

### Digital / Video Images Permission Form

**Parent / Carers Name:** .....

**Student / Pupil Name:** .....

**As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.** **Yes / No**

**I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.** **Yes / No**

**Signed:** .....

**Date:** .....



## Staff (and Volunteer) Acceptable Use Policy Agreement

### School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

#### ***This Acceptable Use Policy is intended to ensure:***

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

### **Acceptable Use Policy Agreement**

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

#### ***For my professional and personal safety:***

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- All data in school is kept securely and staff are informed of what they can and can't do with data through the Online Safety Policy and statements in the Acceptable Use Policy. All data on the school office computer is backed up by LCC Education Digital Services. The school has two computer networks, curriculum and admin. Only the School Bursar and the Headteacher can access the admin network, which is password protected. All other staff and children access the curriculum network, again this is

password protected. The computers in the playroom are logged onto through the children's password and this ensures that the children cannot access any of the staffs' information.

- I will ensure that personal profiles on social media are secure and do not display content that is detrimental to their professional status of the school.
- The two system network is to ensure safety in terms of protecting data. Not only are the networks password protected, but so are important systems like SIMS. This ensures that devices such as smartphones would not be able to access data. Mobile devices such as laptops and encrypted pen drives are allowed to be removed from school in order for professional work to be undertaken from home. Prohibiting this, could detriment the quality of teaching and learning. However, all staff through the acceptable use policy are aware of paramount importance of keeping these devices safe and secure.
- Laptops must not be stored in cars and must be stored in a safe place within school (laptop safe) or a safe place in the home, and must only be used by the member of staff. Pen drives need to be stored securely, ensuring the risk of loss is minimum. Highly sensitive information must not be stored on laptops and pen drives, e.g. safeguarding information, e.g. CAF's. All CAF's are sent via secure email which is password protected and encrypted.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incidents, I become aware of, to the appropriate person.

***I will be professional in my communications and actions when using school ICT systems:***

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with parent/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

**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 e-safety 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.
- 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
- All staff ensure that personal profiles are secure and do not display content that is detrimental to their professional status of the school.

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

- All staff use Outlook 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.
- All school emails include a standard disclaimer at the bottom of all out going email communications.

***The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:***

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. The two system network is to ensure safety in terms of protecting data. Not only are the networks password protected, but so are important systems like SIMS. This ensures that devices such as smartphones would not be able to access data. Mobile devices such as laptops and encrypted pen drives are allowed to be removed from school in order for professional work to be undertaken from home. Prohibiting this, could detriment the quality of teaching and learning. However, all staff through the acceptable use policy are aware of paramount importance of keeping these devices safe and secure.
- Laptops must not be stored in cars and must be stored in a safe place within school (laptop safe) or a safe place in the home, and must only be used by the member of staff.
- I will not use personal email addresses on the school ICT systems. Further information above on the school practice on the use of emails.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. All data in school is kept securely and staff are informed of what they can and can't do with data through the E-Safety Policy and statements in the Acceptable Use Policy. All data on the school office computer is backed up by LCC Education Digital Services. The school has two computer networks, curriculum and admin. Only the School Bursar and the Headteacher can access the admin network, which is password protected. All other staff and children access the curriculum network, again this is password protected. The computers in the playroom are logged onto through the children's password and this ensures that the children cannot access any of the staffs' information.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where

digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

***When using the internet in my professional capacity or for school sanctioned personal use:***

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

***I understand that I am responsible for my actions in and out of the school:***

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.
- **Examples of inappropriate incidents and how they will be dealt with are:**

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

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

**I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.**

**Staff / Volunteer Name:** .....

**Signed:** .....

**Date:** .....



## Acceptable Use Agreement for Community Users

### ***This Acceptable Use Agreement is intended to ensure:***

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

### **Acceptable Use Agreement**

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

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

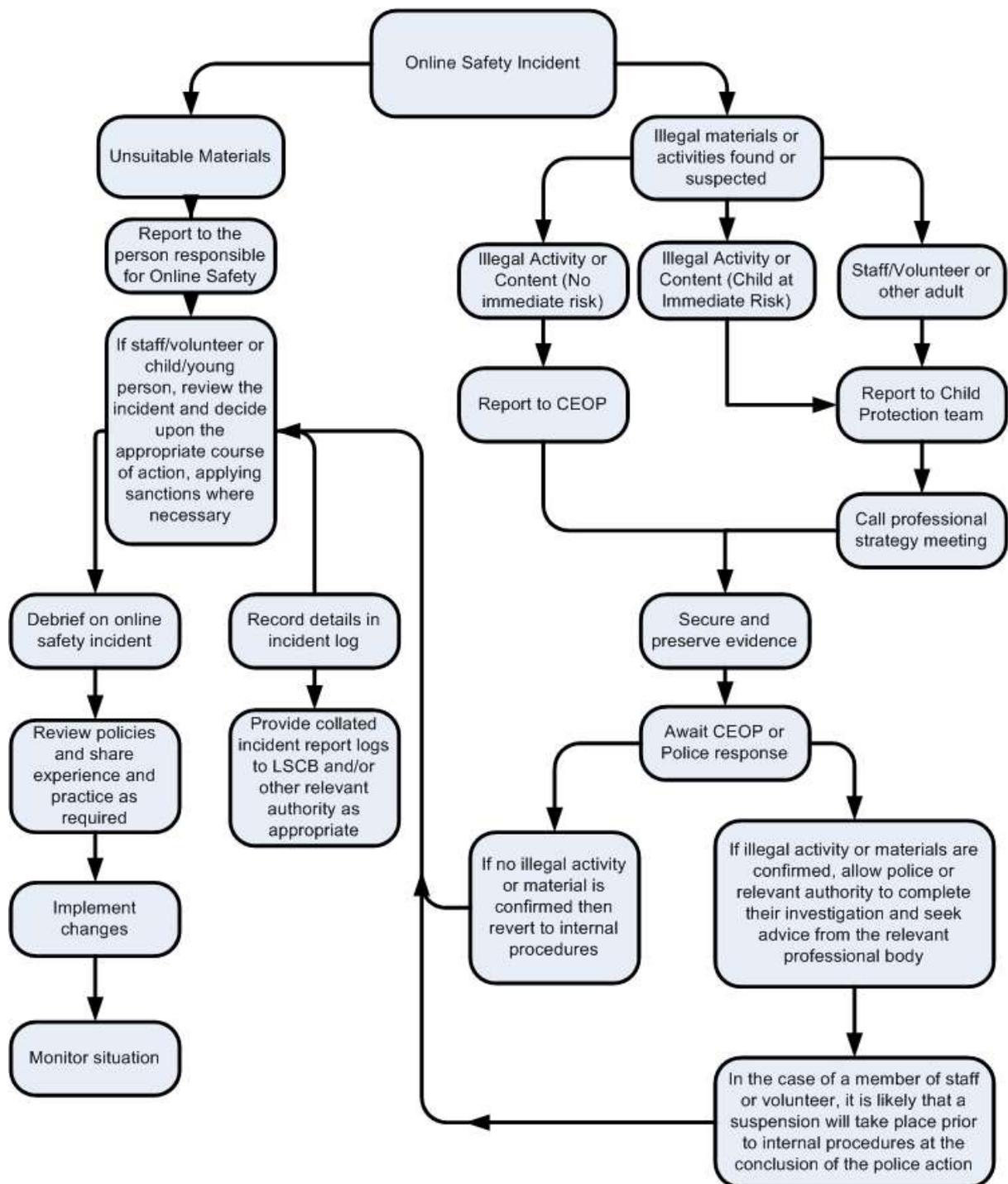
**I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.**

**Name:** .....

**Signed:** .....

**Date:** .....

## Responding to incidents of misuse – flow chart





## Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

### ***Details of first reviewing person***

Name: .....

Position: .....

Signature: .....

### ***Details of second reviewing person***

Name: .....

Position: .....

Signature: .....

### **Name and location of computer used for review (for web sites)**

.....

.....

<b><i>Web site(s) address / device</i></b>	<b><i>Reason for concern</i></b>

### ***Conclusion and Action proposed or taken***

.....

.....

.....

.....

.....

Basnett Street Nursery School

**Reporting Log**

Group: .....

<i>Date</i>	<i>Time</i>	<i>Incident</i>	<i>Action Taken</i>		<i>Incident Reported By</i>	<i>Signature</i>
			<i>What?</i>	<i>By Whom?</i>		

Basnett Street Nursery School

**Training Needs Audit Log**

Group: .....

<i>Relevant training the last 12 months</i>	<i>Identified Training Need</i>	<i>To be met by</i>	<i>Cost</i>	<i>Review Date</i>



## School Technical Security Policy (including filtering and passwords)

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Children have access to the internet in the nursery environment, but this is filtered to a high level, with a filtering system provided by Lancashire County Council.

All data in school is kept securely and staff are informed of what they can and can't do with data through the Online Safety Policy and statements in the Acceptable Use Policy. All data on the school office computer is backed up by LCC Education Digital Services Service. The school has two computer networks, curriculum and admin. Only the School Bursar and the Headteacher can access the admin network, which is password protected. All other staff and children access the curriculum network, again this is password protected. The computers in the playroom are logged onto through the children's password and this ensures that the children cannot access any of the staffs' information.

The two system network is to ensure safety in terms of protecting data. Not only are the networks password protected, but so are important systems like SIMS. This ensures that devices such as smartphones would not be able to access data. Mobile devices such as laptops and encrypted pen drives are allowed to be removed from school in order for professional work to be undertaken from home. Prohibiting this, could detriment the quality of teaching and learning. However, all staff through the acceptable use policy are aware of paramount importance of keeping these devices safe and secure.

### **Responsibilities**

The management of technical security will be the responsibility of [Alison Boyd – School Bursar](#).

### Technical Security

#### Policy statements

The school will be responsible for ensuring that the school 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 receive guidance and training and will be effective in carrying out their responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.** All servers, wireless systems and cabling are securely located. All wireless devices are security enabled and only accessible through a secure password
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.** The School Bursar/Online Safety Champion and Headteacher are responsible for managing the security of the school network.
- **All users will have clearly defined access rights to school technical systems.**
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (*See Password section below*).
- Online Safety Champion is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Mobile device security and management procedures are in place for school provided devices and / or where mobile devices are allowed access to school systems.
  - Staff lockers are used to secure personal mobile phones during the school day for safe storage.
- Mobile phones must only be used on designated breaks and parents and visitors must be
  - prohibited from using them (see mobile phone and social networking policy & visible posters)
- See camera and recording device policy
- I pads are used as a teaching and learning resource in the nursery environment. These are used in line with the security and data management outlined above.
- See above for laptops and pen drives.

## Basnett Street Nursery School

- Walkie Talkies are used to support the organisation, management and safety of children in the outdoor environment. The Walkie Talkies are a digital device, which use a channel that is locked and secure.
- In the event of an emergency – staff, parents and visitors can be contacted through the school office.
- Procedures are in place for reporting any suspicions use of mobile and/or cameras.
  
- 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.
- *Remote management tools are used by staff to control workstations and view users activity*
- *An appropriate system is in place where incidents are recorded in the incident log and reported and audited by the online safety coordinator.*
- An agreed policy is in place (Online Safety Policy) for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- *An agreed policy is in place (Online Safety Policy) regarding the downloading of executable files and the installation of programmes on school devices by users*
- *An agreed policy is in place (Online Safety Policy) regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place (Online Safety Policy) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. (see School Personal Data Policy Template in the appendix for further detail)*
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy in the appendix for further detail)*

### Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

### **Policy Statements**

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by Alison Boyd and will be reviewed, at least annually by SLT.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The “administrator” passwords for the school systems must be available to the *Headteacher* and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.
- All users will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

## Basnett Street Nursery School

- *Passwords for new users, and replacement passwords for existing users will be allocated by the Headteacher. Any changes carried out must be notified to the manager of the password security policy (above).*
- *Users will change their passwords at regular intervals – as described in the staff section below*
- *Where passwords are set / changed manually requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user. Requests by staff member to be authorised and conducted by Headteacher.*

### Staff Passwords

- All staff users will be provided with a username and password by the school's Technical Support Officer provided by LCC Education Digital Services. School Bursar will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- *must not include proper names or any other personal information about the user that might be known by others*
- *the account should be “locked out” following six successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their password, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school*
- should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous password created by the same user. *The last four password cannot be re-used.*

### Pupil Passwords

- Due to the children's age group they do not require an individual username and password however the children will be taught the importance of password security log-ins.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

### Training / Awareness

It is essential that users should be made aware of the need for keeping password secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ins are being used.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

## Basnett Street Nursery School

Pupils will be made aware of the school's password policy:

- in lessons during group time
- through the Acceptable Use Agreement

### Audit / Monitoring / Reporting / Review

The School Bursar will ensure that full manual records are kept of:

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

## Filtering

### Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

### Responsibilities

The responsibility for the management of the school's filtering policy will be held by Online Safety Champion. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- **be reported to the Headteacher and a second responsible person** - Technical Support Officer at LCC Education Digital Services to conduct the necessary changes

All users have a responsibility to report immediately to Online Safety Champion any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

### Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school and LCC Education Digital Services. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

## **Basnett Street Nursery School**

- The school maintains and supports the managed filtering service provided by the Internet Service Provider - LCC Education Digital Services
- The school has provided differentiated user-level filtering through the use of the filtering programme provided by LCC Education Digital Services. Allowing different filtering levels for different groups of users – staff / pupils etc.)
- In the event of the LCC Education Digital Services needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the LCC Education Digital Services and the Headteacher/Online Safety Champion. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

### **Education / Training / Awareness**

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through the induction process / newsletter etc.

### **Changes to the Filtering System**

The school provides:

- request changes to the filtering by reporting to the Online Safety Champion or Headteacher which will be provided by LCC Education Digital Services
- the grounds on which they may be allowed or denied such as social networking sites for some users.
- a second responsible person (Headteacher) to provide checks through inspection of records / audit of logs)
- any audit / reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Online Safety Champion who will decide whether to make school level changes (as above).

### **Monitoring**

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows:

## Basnett Street Nursery School

### Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person - Headteacher
- Online Safety Governor
- External Filtering provider / Local Authority / Police

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

### Further Guidance

Schools in England (and Wales) are required *“to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”* ([Revised Prevent Duty Guidance: for England and Wales, 2015](#)).

Furthermore the Department for Education published [proposed changes](#) to ‘Keeping Children Safe in Education’ for consultation in December 2015. Amongst the proposed changes, schools will be obligated to *“ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system”* however, schools will need to *“be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”*

In response UKSIC produced guidance on – information on [“Appropriate Filtering”](#)  
NEN Technical guidance: <http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/>

Somerset Guidance for schools – this checklist is particularly useful where a school / academy uses external providers for its technical support / security: <https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx>



### School Personal Data Handling Policy

#### **Introduction**

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

#### **Policy Statements**

The school 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".

#### **Personal Data**

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils*, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

## Basnett Street Nursery School

### Responsibilities

The school's Senior Information Risk Officer (SIRO) is Lindsay Ingham. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) as the School Bursar and Headteacher for the various types of data being held (e.g. pupil information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

### Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.:

[http://www.ico.gov.uk/what\\_we\\_cover/register\\_of\\_data\\_controllers.aspx](http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx)

### Information to Parents / Carers – the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through the Prospectus and letter of communication. Parents / carers of young people who are new to the school will be provided with the privacy notice through the Prospectus.

More information about the suggested wording of privacy notices can be found on the DfE website:

<http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn>.

### Training & Awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

### Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

## Basnett Street Nursery School

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

<i>Risk ID</i>	<i>Information Asset affected</i>	<i>Information Asset Owner</i>	<i>Protective Marking (Impact Level)</i>	<i>Likelihood</i>	<i>Overall risk level (low, medium, high)</i>	<i>Action(s) to minimise risk</i>

### Impact Levels and Protective Marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

<b>Government Protective Marking Scheme label</b>	<b>Impact Level (IL)</b>	<b>Applies to schools?</b>
<b>Not Protectively Marked</b>	0	Will apply in schools
<b>Protect</b>	1 or 2	
<b>Restricted</b>	3	
<b>Confidential</b>	4	Will not apply in schools
<b>Highly Confidential</b>	5	
<b>Top Secret</b>	6	

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

## Basnett Street Nursery School

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

### Secure Storage of and Access to Data

The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly (See Online Safety Policy). User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB 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, and
- 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.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

(see appendix for further information and the ICO Guidance: [http://www.ico.org.uk/for\\_organisations/guidance\\_index/~media/documents/library/Data\\_Protection/Practical\\_application/cloud\\_computing\\_guidance\\_for\\_organisations.ashx](http://www.ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx))

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

## **Basnett Street Nursery School**

The school recognises that under Section 7 of the DPA, <http://www.legislation.gov.uk/ukpga/1998/29/section/7> data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

### **Secure transfer of data and access out of school**

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

### **Disposal of data**

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

## Basnett Street Nursery School

### **Audit Logging / Reporting / Incident Handling**

It is good practice, as recommended in the “Data Handling Procedures in Government” document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a “responsible person” for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan.

### **Use of technologies and Protective Marking**

The following provides a useful guide:

	<i><b>The information</b></i>	<i><b>The technology</b></i>	<i><b>Notes on Protect Markings (Impact Level)</b></i>
<b>School life and events</b>	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
<b>Learning and achievement</b>	Individual pupil academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child’s learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not

## Basnett Street Nursery School

		belonging to the parent.	to make this pupil record available in this way.
<b>Messages and alerts</b>	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via “dashboards” of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.



### School Policy: Electronic Devices - Searching & Deletion

#### **Introduction**

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The *Head Teacher* must publicise the school behaviour policy, in writing, to staff, parents / carers and pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

#### **Responsibilities**

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies

## Basnett Street Nursery School

may be delegated to other individuals or groups. The policies will be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Headteacher – Lindsay Ingham  
The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

- Lead Teacher
- School Bursar

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

### Training / Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

## Basnett Street Nursery School



### Mobile Technologies Policy

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

The absolute key to considering the use of mobile technologies is that the pupils, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of policies including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

#### **Potential Benefits of Mobile Technologies**

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen children learning, but they can also develop digital literacy, fluency and citizenship in children that will prepare them for the high tech world in which they will live, learn and work.

For further reading, please refer to "Bring your own device: a guide for schools" by Alberta Education available at:

<http://education.alberta.ca/admin/technology/research.aspx> and to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - <http://www.nen.gov.uk/bring-your-own-device-byod/>

#### **Considerations**

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

## Basnett Street Nursery School

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school Acceptable Use Agreements for staff, parents/carers will give consideration to the use of mobile technologies
- The school allows:

	<b>School Devices</b>			<b>Personal Devices</b>		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device <sup>1</sup>	Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No <sup>2</sup>	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	Yes	Yes
No network access				No		

- **The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices:**
  - All school devices are controlled through the use of Mobile Device Management software
  - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
  - The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
  - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
  - Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
  - *All school devices are subject to routine monitoring*
  - *Pro-active monitoring has been implemented to monitor activity*
  
- **When personal devices are permitted:**

---

<sup>1</sup> Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

<sup>2</sup> The school should add below any specific requirements about the use of personal devices in school, e.g. storing in a secure location, use during the school day, liability, taking images etc

## Basnett Street Nursery School

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues
- **Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition:**
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
  - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in school
  - Devices must be in silent mode on the school site and on school buses
  - School devices are provided to support learning.
  - Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - The changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted
  - The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
  - The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not

## Basnett Street Nursery School

be accessible to children on authorised devices once they leave the school roll.  
Any apps bought by the user on their own account will remain theirs.

- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- *Devices may be used in lessons in accordance with teacher direction*
- *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*
- *Printing from personal devices will not be possible*

## Basnett Street Nursery School



### Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn, Youtube) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities, which, a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

#### **Scope**

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications, which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. 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.

#### **Organisational control**

#### **Roles & Responsibilities**

- SLT

## Basnett Street Nursery School

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts
- Approve account creation
  
- **Administrator / Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
  
- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts
  - Adding an appropriate disclaimer to personal accounts when naming the school

### Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a “Friends of the school” Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training.

### Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

## Basnett Street Nursery School

### Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

### Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

### Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

### Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging

## Basnett Street Nursery School

- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

### Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

### Personal use

- **Staff**
  - Personal communications are those made via a personal social media accounts. 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.
- **Pupil**
  - Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.
  - The school's education programme should enable the pupils to be safe and responsible users of social media.
  - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
  - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.

## Basnett Street Nursery School

- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

### Monitoring posts about the school

- 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.

## Appendix

### Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

### Managing school social media accounts

#### The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

## Basnett Street Nursery School

### The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

## Basnett Street Nursery School

### Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an e safety issue or situation.

#### **Computer Misuse Act 1990**

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

#### **Data Protection Act 2018**

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

#### **Freedom of Information Act 2000**

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

#### **Communications Act 2003**

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

#### **Malicious Communications Act 1988**

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

## Basnett Street Nursery School

### **Regulation of Investigatory Powers Act 2000**

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

### **Trade Marks Act 1994**

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

### **Copyright, Designs and Patents Act 1988**

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

### **Telecommunications Act 1984**

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

### **Criminal Justice & Public Order Act 1994**

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

## Basnett Street Nursery School

### **Racial and Religious Hatred Act 2006**

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### **Protection from Harrassment Act 1997**

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

### **Protection of Children Act 1978**

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

### **Sexual Offences Act 2003**

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

### **Public Order Act 1986**

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

### **Obscene Publications Act 1959 and 1964**

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

### **Human Rights Act 1998**

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination

## Basnett Street Nursery School

- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

### **The Education and Inspections Act 2006**

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

### **The Education and Inspections Act 2011**

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

### **The Protection of Freedoms Act 2012**

Requires schools to seek permission from a parent / carer to use Biometric systems

### **The School Information Regulations 2012**

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

### **Serious Crime Act 2015**

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

## Basnett Street Nursery School



### Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

#### **UK Safer Internet Centre**

Safer Internet Centre – <http://saferinternet.org.uk/>

South West Grid for Learning - <http://swgfl.org.uk/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Internet Watch Foundation - <https://www.iwf.org.uk/>

#### **CEOP**

CEOP - <http://ceop.police.uk/>

**ThinkUKnow** - <https://www.thinkuknow.co.uk/>

#### **Others**

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) - [www.education.gov.uk/ukccis](http://www.education.gov.uk/ukccis)

Netsmartz - <http://www.netsmartz.org/>

#### **Tools for Schools**

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

#### **Bullying / Cyberbullying**

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance - [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/374850/Cyberbullying\\_Advice\\_for\\_Headteachers\\_and\\_School\\_Staff\\_121114.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf)

Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - <http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work>

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

#### **Social Networking**

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

Reviewed April 2021

## **Basnett Street Nursery School**

### [Facebook Guide for Educators](#)

### **Curriculum**

[SWGfL Digital Literacy & Citizenship curriculum](#)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.eu/)

Insafe - [Education Resources](#)

### **Mobile Devices / BYOD**

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

### **Data Protection**

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)

[ICO - Guidance we gave to schools - September 2012 \(England\)](#)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

[Information Commissioners Office good practice note on taking photos in schools](#)

[ICO Guidance Data Protection Practical Guide to IT Security](#)

[ICO – Think Privacy Toolkit](#)

[ICO – Personal Information Online – Code of Practice](#)

[ICO Subject Access Code of Practice](#)

[ICO – Guidance on Data Security Breach Management](#)

SWGfL - [Guidance for Schools on Cloud Hosted Services](#)

LGfL - [Data Handling Compliance Check List](#)

Somerset - [Flowchart on Storage of Personal Data](#)

NEN - [Guidance Note - Protecting School Data](#)

### **Professional Standards / Staff Training**

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs](#)

[Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

### **Infrastructure / Technical Support**

Somerset - [Questions for Technical Support](#)

NEN - [Guidance Note - esecurity](#)

### **Working with parents and carers**

[SWGfL Digital Literacy & Citizenship curriculum](#)

[Online Safety BOOST Presentations - parent's presentation](#)

[Connectsafely Parents Guide to Facebook](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

Reviewed April 2021

## **Basnett Street Nursery School**

[Teach Today - resources for parents workshops / education](#)

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

### **Research**

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

[Ofcom – Children & Parents – media use and attitudes report - 2015](#)

## Basnett Street Nursery School



### Glossary of Terms

<b>AUP / AUA</b>	Acceptable Use Policy / Agreement – see templates earlier in this document
<b>CEOP</b>	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
<b>CPD</b>	Continuous Professional Development
<b>FOSI</b>	Family Online Safety Institute
<b>ES</b>	Education Scotland
<b>HWB</b>	Health and Wellbeing
<b>ICO</b>	Information Commissioners Office
<b>ICT</b>	Information and Communications Technology
<b>ICTMark</b>	Quality standard for schools provided by NAACE
<b>INSET</b>	In Service Education and Training
<b>IP address</b>	The label that identifies each computer to other computers using the IP (internet protocol)
<b>ISP</b>	Internet Service Provider
<b>ISPA</b>	Internet Service Providers' Association
<b>IWF</b>	Internet Watch Foundation
<b>LA</b>	Local Authority
<b>LAN</b>	Local Area Network
<b>MIS</b>	Management Information System
<b>NEN</b>	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
<b>Ofcom</b>	Office of Communications (Independent communications sector regulator)
<b>SWGfL</b>	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
<b>TUK</b>	Think U Know – educational online safety programmes for schools, young people and parents.
<b>VLE</b>	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
<b>WAP</b>	Wireless Application Protocol
<b>UKSIC</b>	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in April 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.