



# **ONLINE SAFETY POLICY 2025-2026**

## **BROOMHALL AND GRACE OWEN NURSERY SCHOOL**

# Online Safety Policy 2025-2026

## The Acceptable Use of Internet and Related Technologies Policy

### Broomhall and Grace Owen Nursery Schools

#### **Aim of this policy:**

Our prime responsibility is the welfare and wellbeing of all children in our care. This policy is produced to define procedures and staff practices at the nursery to prevent the misuse of IT. We are committed to promoting online safety. Please see information which is available to all parent / carers on our website, as well as our Safeguarding Policy.

Within this policy we will be outlining the agreed procedures for using:

- Digital cameras
- Staff mobiles and smart watches
- The internet
- Screen time
- Social networking

We are aware that technology is continuously developing and this policy will be reviewed accordingly.

For information about children's use of technology please see Appendix A.

#### **Principles:**

- Any information an educator comes into contact is regarded as being confidential.
- In particular sensitive information relating to a child or their parent / carer should only be shared on a 'need to know' basis.
- Families consent must always be sought to share information, including when making referrals to other professionals, unless it is thought unsafe to do so.
- If a practitioner makes a written record relating to an incident with a child, or family, then the parents / carers should be informed, unless it is thought unsafe to do so. Please remember keeping records a secret from families may result in evidence becoming inadmissible if those records are then used in a court of law in a child abuse case.
- Practitioners should also remember when they write anything about a child or family that the General Data Protection Regulations (GDPR) gives them the right to request to see all the information we hold on that child.
- If a practitioner is worried about information they have come into contact with they should share this with the Headteacher at the first available opportunity.
- We are legally obliged to share confidential information without authorisation from the person who provided it, or to whom it relates, if it is in the public interest. That is when: - It is to prevent a crime from being committed or to intervene where one may have been, or to

prevent harm to a child or adult; or – Not sharing it could be worse than the outcome of having shared it.

- The decision to share information should never be made as an individual, but with the backup of the colleagues and the Headteacher.
- All students, volunteers and new starters in the setting should be asked to read this policy and agree to abide by its limitations.
- In nurseries we encourage all adults and children to develop their protective behaviours. This means everyone has the right to feel safe at all times. Support should always be available from the management team.

## **Roles and Responsibilities**

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for Online Safety has been designated to a member of the senior leadership team.

Our school Online Safety Co-ordinator is **Kirsty Bray (Grace Owen)/ Natalie Cullum (Broomhall)**.

Our school Designated Safeguarding Lead is **Leonie Matthews (Grace Owen)/ Natalie Cullum (Broomhall)**.

The School's Online Safety Coordinator ensures they keep up to date with Online Safety issues and guidance through liaison with the Local Authority Online Safety Officer and through organisations such as London Guide for Learning, CASPAR, and The Child Exploitation and Online Protection (CEOP). The school's Online Safety coordinator ensures the Headteacher, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of Online Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-safety and are updated at least annually on policy developments.

All teachers / practitioners are responsible for promoting and supporting safe behaviours in the nursery and follow school Online Safety procedures.

## **Protecting Confidential Information:**

- All confidential information must be stored in either locking filing cabinets / cupboards or on nursery computers. This information should never be taken home by practitioners. Computers are password encoded with two factor authentication and only practitioners are in possession of the password.
- Confidential data includes personal data such as names, addresses, dates of birth, bank details, national insurance numbers and qualifications.
- Development records, photos, accident, incident, administration of medication records and any records kept for the purpose of child protection are also confidential.

- To ensure that we are meeting the requirements of the General Data Protection Regulations (GDPR) we are registered with the Information Commissioner's Office. (please see Data Protection Policy for more information).

### **Access to Personal Records:**

Parents may request access to any records held on their child and family following the procedure below.

- Any request to see the child's personal information by a parent or person with parental responsibility must be made in writing to the Headteacher.
- The Headteacher sends a written acknowledgement.
- The nursery commits to providing access within 14 working days, although this may be extended.
- The Headteacher prepares the file for viewing.
- All third parties are written to, stating that a request for disclosure has been received and asking for their permission to disclose to the person requesting it. A copy of these letters is retained on the file.
- 'Third parties' include all family members who may be referred to in the records. It also includes workers from any other agency, including social services, the health authority, etc. it is usual for agencies to refuse consent to disclose, preferring the individual to go directly to them.
- When all the consents / refusals to disclose have been received these are attached to the copy of the request letter.
- A photocopy of the complete file is taken.
- The Headteacher goes through the file and removes any information which a third party has refused consent to disclose. This is best done with a thick black marker, to score through every reference to third party and information they have added to the file.
- What remains is the information recorded by the nursery, detailing the work initiated and followed by them in relation to confidential matters. This is called the 'clean copy'.
- The 'clean copy' is photocopied for the parents who are then invited in to discuss the contents. The file should never be given straight over but should be gone through by the Headteacher so that it can then be explained.
- Legal advice may be sought before sharing a file, especially where the parent has possible grounds for litigation against the nursery or another (third party) agency.

All the undertakings above are subject to the paramount commitment of the nursery, which is to ensure the safety and well-being of the child. Please refer to the Safeguarding Policy.

### **Digital Safety:**

The world is changing rapidly and the emergence of the internet and, over the past decade, social media has had an effect on all of our lives. Used safely it can be a powerful tool for learning and connection across the globe, however we must also take steps to ensure it keeps children and adults safe.

## Social Media and Social Networking

### What is Social Media?

Social media is the term commonly used for websites which allow people to 'network' and interact with each other by sharing information, opinions, knowledge and interests.

Here are some of the main 'types' of social media websites: •

- Social networking – services that allow you to interact with other people of similar interests and backgrounds, ability to add friends, comment on profiles, join groups and have discussions e.g. Facebook, LinkedIn, etc.
- Social bookmarking sites – services that allow you to interact by tagging websites, search through websites booked marked by other people and share these e.g. Blinklist and StumbleUpon.
- Social news – services that allow you to interact by voting for articles and commenting on them e.g. Digg and Reddit.
- Social media sharing – services that allow you to interact by sharing photos or videos and commenting on profiles and user submissions e.g. YouTube, Flickr, Instagram, Pinterest, etc.
- Microblogging – services that focus on short updates that are pushed out to anyone subscribed to receive updates e.g. Twitter / X.
- Blogging / forums – services that allow you to post a comment and reply to other comments, thus developing discussions. In both cases, you can leave comments which may or may not be moderated and you may have to identify yourself with a name and email address.

Staff are asked to use social media and social networking sites with caution. There must be no mention of the nursery schools, nor should any anecdotal incidents be repeated in the public domain. Nor should it be used for communication between staff and parents. We ask that all staff adhere to our confidentiality policy. To support this we ask that our families do not attempt to contact or communicate with members of staff through social media or social networking sites.

- We expect practitioners to uphold the same standards of behaviours in both their online and offline lives.
- We expect practitioners to make a clear division between their personal and private lives. Practitioners will not identify themselves as working for Sheffield city council nurseries, or post pictures taken in the nursery or whilst at work.
- We expect practitioners to assume that any material, thoughts or images they publish online are public and will be shared widely.
- Practitioners must not engage in illegal online activity, or bring the setting into disrepute.
- Practitioners should never name or identify children or the families attending the nursery through the material they post online.
- Practitioners must make clear that views expressed in their own online space are their own and not necessarily those of their employer.
- Practitioners must never publish documents or materials belonging to the nursery online; this includes photos of the children. This requirement continues even after they have left employment at the nursery.

- Practitioners must not use professional email addresses to set up personal social media accounts. They should also be aware that online activity taking place at the setting can be traced back to the setting IP address and therefore they must be considerate of any online activity they engage in whilst at work, such as editing Wikipedia.
- Practitioners must refuse friend requests from parents or other family members on Facebook or similar sites. Practitioners are likewise expected to defriend any new starters they have existing friendships with via social media.
- We accept that practitioners will maintain social media friendships with co-workers and family members using the setting. Any such friendship should be declared within supervision. However we expect that they will not use information about the setting for personal gain, or to bring the setting into disrepute.
- Practitioners must not befriend children who have previously attended the setting via social media. This behaviour could be considered grooming.
- We advise caution when befriending other staff members / volunteers over social media.
- Practitioners will refuse friend requests from college students until they have completed their placements at the setting.
- Once they have left the setting practitioners must not contact nursery parents via social media. Likewise they must not contact families of settings that they have left the employment of via social media. This may affect any future references that the individual may request.

#### Parents and Families:

- We request that parent's respect our rules around social media and do not attempt to make contact / friend staff online.
- We expect that parents will not abuse the setting or make false statements about the setting online. If this does happen, all childcare arrangements may be terminated without prior warning.
- We would request that parents do not identify their children as attending the setting, take photos whilst at the nursery or share photos of other family's children online.
- We ask that you read Appendix A for keeping your child safe online.

#### iPads and Tablets:

The setting has iPads and tablets solely for the use within the setting. Photographs (and videos) are taken for the purpose of monitoring the child's development and as a visual representation of their time at nursery. Occasionally some photos may be used for other purposes. As part of the registration process parent / carers are requested to tick photograph consents which give them options concerning media use for their nursery website, press, and other nursery publicity or research. The nursery iPads and tablets do not leave the nursery premises and are locked away overnight. Practitioners are not permitted to take photographs on personal cameras or mobile phones (see section below) of the children anywhere in the setting.

#### Safeguarding:

Any staff member has a right to challenge any other member of staff regarding their media use and is obligated to report any concern immediately to the Designated Safeguarding Lead. At the discretion

of the Designated Safeguarding Lead, the suspected member of staff may be required to leave the setting immediately and their iPad / phone / tablet retained for further investigation. For more information, please refer to the setting's Safeguarding Policy.

### **How will complaints regarding Online Safety be handled?**

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access. Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying are dealt with in accordance with our **Anti-Bullying Policy**. Decisions on appropriate use of content, images, communications or behaviour shall be consistent with our Safeguarding Policy.

### **References**

**The relevant legislations, standards and guidance used as a framework for this policy and the procedures are:**

- General Data Protection Regulations (2018)
- Human Rights Act (1998)
- The Regulation of Investigatory Powers Act (2000)
- Information sharing: Guidance for Practitioners and Managers (DCSF 2008)

**Additional information from KCSIE September 2025 will be added when available. It will include the use of AI**

## Appendix A

### Children Online

#### What young children are doing online

Children in the early years are using digital devices more. According to the [2024 Ofcom](#) report 85% of children aged 3 to 4 are using apps like YouTube.

Research shows that children are watching video-on-demand content on video-sharing platforms rather than television, such as cartoons, mini movies and songs. However, unlike older children, only a small number of children aged 3 to 4 (23%) play games online

#### How device use can affect development

Screen use can benefit children's development in the early years but there are challenges that you should be aware of. Ongoing research suggests there are both positive and negative developmental outcomes

#### Benefits

Screen use (depending upon how it is used) can support young children in your care by:

- providing opportunities to promote creativity and learning
- encouraging language development
- improving numeracy and literacy skills
- creating a greater understanding of their world
- developing their digital skills

#### Screen time advice

The World Health Organisation's (WHO) guidance from 2019 on [physical activity, sedentary behaviour and sleep for children under 5 years of age](#) states that to grow up healthy, children need to sit less and play more.

WHO has the following recommendations for screen time:

- under 1: screen time is not recommended
- 1-year-olds: sedentary screen time (such as watching TV or videos, playing computer games) is not recommended
- 2-year-olds: sedentary screen time should be no more than 1 hour; less is better
- age 3 to 4: sedentary screen time should be no more than 1 hour; less is better

#### Using devices in our setting

Electronic devices at Broomhall and Grace Owen Nursery Schools are used as a tool to support children's learning and development.

Children are always closely supervised when using electronic devices.

These websites and apps have educational content appropriate for early years children:

- [CBeebies Little Learners app](#): Free games and video activities.
- [Teach Your Monster](#): Free games to teach children reading, number skills and adventurous eating.
- [Cosmic Kids Yoga](#): Free yoga videos for children, turning screen time into physical activity.

Sometimes there may be an education reason to watching a video on YouTube, for example, looking at whales in their natural environment to support a story the children are learning. All YouTube videos are always viewed via [YouTube Kids](#).

### **Access technology safely**

We support children's use of technology in our setting by:

- informing parents and carers and early years staff members on how to support children's use of technology
- using device safety settings to ensure apps and content are age-appropriate
- monitoring and supporting children while they use devices
- thinking about what we post online and how this may impact our role or children in our care
- getting parental consent before creating or sharing images of children and store them safely

### **Teach and share internet safety guidelines**

Talk to parents and carers, and young children about internet safety. You can:

- help young children understand what safe use of technology looks like
- have conversations and share advice with parents and carers to encourage safe online use in the home
- stay up to date with issues that young children face online through [online safety training](#)
- keep up to date with [news and research on internet safety](#)