

The University of Warwick Nursery

E- Safety Policy

Online Safety in the Early Years is vital in keeping children safe from harm whilst watching online content and is recognised as part of the setting's Safeguarding responsibilities.

Prevent Duty (2015)

- **Schools (and registered childcare providers) 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.**
- **Ofsted ‘Inspecting Safeguarding’ 2018: Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children’s well-being.**

By implementing a comprehensive online safety policy, the University of Warwick Nursery can help protect children and promote their safe and positive use of technology. Guidelines for using technology in Early Years settings focuses on supervision, appropriate content and communication with parents and children. All risks and benefits of online activities for children are regularly reviewed and updates take place. Staff model appropriate behaviour and boundaries in regard to using technology in their everyday practice ensuring all children are safe from harm.

The University of Warwick Nursery's online safety policy covers a variety of different aspects of all online activity including the use of personal devices, wearable technology, mobile phones and cameras, technology used in the setting, expectations regarding professional boundaries and behaviours of staff including communication via social media.

Online Safety at nursery

Staff are permitted to use the internet on the nursery laptops for the educational benefit of the children. This may be for gathering information, using Twinkl, playing music, using Microsoft Word for observations or iConnect. Staff are prohibited from using the nursery laptops for personal use.

The settings Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (DDSL) take responsibility for online safety concerns within the setting.

Our DSL is:

- **Jo Warren, Nursery manager**

Our DDSLs are:

- **Debbie Pinkerton, Assistant Manager**
- **Donna Egan, Claire Carey and Carole Rawlinson, Senior Early Years Educators.**

‘Keeping children safe in Education’ (KCSIE) states that:

‘The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder’s job description’.

DSL will:

- Holds the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and updated training on online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Report directly to their line manager if online safety has been compromised, ensuring all incidents are recorded.

Staff will:

- Not use personal devices such as laptops, mobile phones etc to show children online content. (See Camera and Mobile Phone Policy)
- Not leave the room laptop where children can access it without adult supervision.
- Share with parents’ photos and videos of their children only on the Parents Zone using the nursery iPad and iConnect.

Parents and visitors to the nursery will be asked:

- Not to use their mobile phones or laptops in the atrium or in the playrooms within the nursery. They can be used whilst sitting on the chairs in reception (See Camera and Mobile Phone Policy).
- Not to share photos and videos of other people’s children, taken outside the nursery, on their social media accounts unless they have permission from the other children’s parents.
- To share with staff any information that would support online safety within the nursery.
- Not allowed to use wearable technology such as video glasses within the nursery without informing the staff. Parents will be asked to remove these devices before entering the nursery.

Use of Devices in the Early Years

The Government Department for Education has a document entitled ‘Internet Safety’ <https://help-for-early-years-providers.education.gov.uk/health-and-wellbeing/internet-safety>. They give helpful advice and information regarding using devices for internet use in the early years of a child’s development.

They state:

“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

Challenges

Screen use in the early years can have an impact on a young child's development. It can:

- impact their ability to control their emotions
- impact how they deal with social interactions and activities
- expose them to inappropriate content

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

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

Social media and networking

The University of Warwick Nursery accepts that staff and parents use social media sites. This policy sets out the mandatory requirements for social media users:

1. When using social media sites, no reference should be given to the nursery, specific children or parents by name.
2. No pictures taken at the nursery setting should be published on personal social media pages.

3. Staff should not accept 'friend requests' from parents or 'follow' parents on social media websites.
4. Social media sites should not be accessed from a nursery computer.
5. Staff may access their own social media pages from their own phones but only during their agreed breaks when children are not present.
6. Do not make disparaging remarks about your employer/colleagues. Doing this may be deemed as bullying and/or harassment and would be subject to the University Dignity at Work policy.
7. If you have any concerns about information on your social networking site or if you are the victim of cyberbullying, you should contact the nursery manager, the Director of The People Team or the nursery HR advisor immediately.

In addition, the University of Warwick Nursery does not have an independent social media account.

Summary of the actions taken to protect children when online.

- **Supervision:**

Children are always closely supervised when using technology. The staff only have internet access on the playrooms' laptops and the whiteboard in the atrium. The children cannot gain access to a setting's laptop without adult supervision. Laptops are put out of reach of children when not being used by an adult.

- **Appropriate Content:**

Websites and search results are carefully selected and checked to ensure they are age-appropriate and safe by one of the 4 DSLs. Staff ask parents for links and addresses to programmes in foreign languages for children to watch at nursery.

- **Modelling Safe Practices:**

Practitioners model safe internet use and language when using technology with children. Never use personal devices with children in the setting. Consider the importance of digital literacy for both children and staff.

- **Parent Communication:**

Inform parents about online safety risks and the importance of monitoring their children's online activities. Remind parents of the importance of setting age-appropriate time limits for children's screen time. Share with parents the guide for parents and carers entitled 'Young children and screen time- a good start'.

- **Data Protection:**

Ensure that data is shared online in accordance with the setting's data protection responsibilities.

- **Regular Review and Updates:**

The policy should be reviewed and updated regularly to reflect changes in technology and best practices.

- **Training:**

Staff should be trained on online safety and how to keep children safe online. During staff meetings, our E-Safety Champion will deliver training to all staff, keeping E-Safety at the front of their knowledge.

- **Use of IT Equipment:**

Ensure staff only use IT equipment for matters relating to the children's education and care and not for personal use. Privacy and safety settings are set at the highest level.

Other University of Warwick Policies relating to this subject include: ***Camera and Mobile phone policy*** and ***Data Protection Policy***

Internet use and computers

Staff are permitted to use the internet on the nursery laptops for the educational benefit of the children. This may be for gathering information, images or to use an age appropriate learning programme or video footage for the children. Staff are prohibited from using the nursery laptops for personal use. The following points must also be adhered to:

- Staff must ensure there is a password lock on the device at all times when it is not being used;
- Staff are not permitted to leave a child unattended on a computer at any time;
- All videos that are shown to the children should be watched in full by the member of staff concerned to ensure the content is appropriate;
- All images shown to the children should be viewed in advance to ensure it is appropriate;
- Staff are not permitted to browse the internet whilst children are present.

Complaints of internet misuse including a breach of the above contract should be reported to the settings DSLs immediately. If these concerns are of a safeguarding nature they will be dealt with in accordance with the Safeguarding Policy. Debbie reserves the right to monitor any internet sites visited.

Staff may access the internet for personal use via their smart phones in their own time and only during their staff breaks. Children should not be present during this time.

Electronic mail

E-mail is a useful way to communicate with parents about their child and current activities at the nursery. E-mail can be used by staff for work purposes, but information must be sent through the nursery's email account, nurseryenquiries@warwick.ac.uk. Staff who wish to send information via the nursery email account must obtain strict permission from the manager.

E-mailing of personal, sensitive, confidential or a classified nature should be avoided but, if necessary, staff should obtain specific content consent from Jo Warren. Any email sent that contains personal data, including names, or any other detail that could identify a child or their parent must be encrypted.

Staff must not contact parents whose children attend the setting using their personal email accounts, social media platforms, nor give out their personal email addresses.

Social media and networking

The University of Warwick Nursery accepts that staff and parents use social media sites. This policy sets out the mandatory requirements for social media users:

1. When using social media sites, no reference should be given to the nursery, specific children or parents by name.
2. No pictures taken at the nursery setting should be published on personal social media pages.
3. Staff should not accept 'friend requests' from parents or 'follow' parents on social media websites.
4. Social media sites should not be accessed from a nursery computer.
5. Staff may access their own social media pages from their own phones but only during their agreed breaks when children are not present.
6. Do not make disparaging remarks about your employer/colleagues. Doing this may be deemed as bullying and/or harassment and would be subject to the University Dignity at Work policy.
7. If you have any concerns about information on your social networking site or if you are the victim of cyberbullying, you should contact the nursery manager, the Director of The People Group or the nursery HR advisor immediately.

In addition, the University of Warwick Nursery does not have an independent social media account. All social media activity is monitored centrally through the Internal Communications department.

Photography and video recording

Taking pictures or video recordings of children is necessary as it provides evidence of how each child meets the Learning and Development requirements of the EYFS. Parents are however asked to complete the photography and video filming permission part of their registration form to indicate if images or video recordings of their child can be used for any other purposes such as displays or advertising. Staff are responsible for ensuring these wishes are met. Staff must adhere to the following statements:

- a) Pictures and video recordings can only be taken on the nursery cameras
- b) Nursery cameras, including children's cameras, must only be used to record nursery activities of the children;
- c) Under no circumstances can a member of staff use their own electronic device;
- d) Images and recordings can only be of a single child when being used in children's Learning Journals;

- e) The pictures/video recording must be uploaded onto a single memory stick that is only shared between staff and the parent of child. This must be completed within one week and all images/recordings should be deleted from the nursery computer and camera within the same time frame;
- f) There is no reasonable explanation for taking photographs/recordings of children during intimate care routines and so this must not take place;
- g) The processing of photographs should only take place on nursery premises;
- h) The only exception whereby staff can take photographs/videos on a different device is during forest school sessions and outings. Staff can use their own phone camera if a nursery mobile phone is not available but the same procedure, as stated above, applies.

Parents/visitors are asked:

- Not to wear Meta Glasses/ AI Glasses in Nursery. These glasses have the ability to record, take photos and connect to the internet.
- Not to take any photographs or video recordings of children using a laptop or mobile phone while on the nursery premises.
- The only exception to this rule is during special events such a graduation or the Christmas party. Staff remind parents and families only to take photos of their child and no other. Parents are asked not to publish any photographs of other people's children on any social media websites. A great way to do this is to take a photo of your own child with Father Christmas when receiving a present and when receiving graduation certificates from a member of staff. This will ensure that only the staff member and your child is in the photo.

Any member of staff, including volunteers and agency staff in breach of this policy will be subject to disciplinary action. All staff are responsible for reporting any concerns to the setting's DSLs.

Mobile phones

It is not acceptable that staff should be using mobile phones to make or receive phone calls while working directly with the children.

We are therefore imposing the following mandatory expectations on all members of staff, students, agency staff and volunteers;

- Mobile phones are not to be taken into nursery playrooms for any reason, unless given specific permission by the most senior member of staff and only under specific conditions, such as waiting for a call from a health practitioner.
- Staff who need to make or receive emergency phone calls during their working hours (excluding lunch breaks) must do so through the nursery office;
- All mobile phones must be kept in staff lockers in the staff room;
- Mobile phones must not be used to take photographs of the children under any circumstances other than those noted in h) above.

Parents/visitors are asked:

- Not to use their mobile phones to make or receive phone call while on the nursery premises;
- Not to use their mobile phones to take photographs of children, including their own child while on nursery premises.

Use of mobile phones when on outings outside the nursery's boundaries.

- The nursery provides a nursery mobile phone for staff to use when taking children on an outing or to the forest school.
- This phone is preprogrammed with the nursery office number and the emergency call number which connects directly to the university security team.
- The nursery mobile phone should only be used for the purpose of contacting the nursery office or the security and for no other purpose.
- The camera on the mobile phone may only be used to gather evidence of the outing. Strict procedures, as stated above, should be adhered to in relation to storing the images/recordings.

Any member of staff violating these conditions will be disciplined under the gross misconduct clause of their contract. Any member of staff witnessing another member of staff violating this policy must report the violation to the nursery manager in accordance with our safeguarding and professional abuse policies.

The implementation of this policy is made in conjunction with our Professional Abuse policy and Safeguarding Children policy.

CCTV

There are two CCTV cameras in the Nursery that are used as a security measure; the cameras are situated in the main entrance and the atrium. The positioning of the cameras protects children's privacy as they are not situated in the individual rooms. George Saxon, the Systems Manager, is responsible for auditing, servicing and erasing images; images are erased after 28 days. Trained staff (DBS certified) within the Campus safety Team are responsible for the monitoring of the CCTV cameras.