Nottingham Nursery School & Training Centre

E-safety policy

Updated September 2020

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us and our families to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the contents of the *Statutory Framework for the EYFS*.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

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

The safeguarding governor who oversees online safety is Lynette Randall.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The head teacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding leads (DSL) and assistant DSLs are set out in our child welfare and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, schools IT and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Head Teacher (supported by Schools IT)

The Head Teacher (supported by Schools IT) is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring that the security of the school's ICT system are checked and monitored on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure that they have read, understand and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online and on appropriate and safe use of screen-based technology from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf and http://www.childnet.com/resources/keeping-under-fives-safe-online
- NSPCC: Online safety for under 5s https://www.nspcc.org.uk/globalassets/documents/advice-and-info/online-safety-under-5s.pdf
- Internet Matters – Pre-school resources https://www.internetmatters.org/advice/0-5/resources/
- www.actionforchildren.org.uk – *How much time should I let my child spend watching a screen* and *5 tips to unplug and play*

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. They will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils

Pupils will be taught about online safety as part of the curriculum.

As addition to what is taught as part of the EYFS 'Technology' curriculum, pupils will:

- only use technology alongside an adult who will teach them:
  - to use technology safely and respectfully
  - to report anything which concerns them to a trusted adult

5. Educating parents about online safety

The school will raise parents' understanding and awareness of internet safety. This policy will also be shared with parents.

Parents will be offered opportunities to learn about:

- Understanding how changes in technology affect safety, including new ways to protect online privacy and identity
- How to report a range of concerns
- Safe use of social media and the internet for themselves and their children.
- The dangers that can be encountered online including those of Child Sexual Exploitation and Cyber-bullying
- How to use screen-based technology appropriately with the under 5s including the developmental impact and potential dangers of allowing young children to spend long or unsupervised periods online

This will be achieved by providing:

- Information leaflets about e-safety within the parent's area
- Regular e-safety sessions led by family learning and/or members of school staff
- E-safety information shared with parents through the school's social media pages and via letters sent home
- Advice and guidance during parents' meetings

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

Information about cyber-bullying will be included as part of parent learning opportunities.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover development of skills relating to prevention of cyber-bullying. This includes through the PSED curriculum, and other subjects where appropriate.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, this should be reported to the DSL who will make decisions about how to respond and record details of the incident and the response in the Online Safety Incident Report Log (Appendix 4). Where illegal, inappropriate or harmful material has been spread among pupils or families, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Use of mobile devices in school

Pupils are not allowed to bring mobile devices into school and any breach of this agreement will result in the temporary confiscation of their device.

Parents are not allowed to use or get out their mobile devices into school and any breach of this agreement will result in them being asked to put the device away. If parents refuse to put away their device, they will not be allowed to enter the nursery school part of the building. Parents will be expected to sign an agreement to this effect before their children are enrolled.

See the safeguarding policy and staff code of conduct in relation to staff use of personal mobile devices.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device or if they lose their device, they must seek advice from the head teacher.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate information as part of their induction.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

Parent/carer agreement:

If I bring a personal mobile phone or other personal electronic device into school:

- I agree not to use it or have it out on display whilst I am in the nursery setting.
- I will not take photographs anywhere on the School site without the expressed permission of a member of staff.
- If I use my personal mobile phone or other personal electronic device to take photos or video clips during school events and performances (with the expressed permission of the supervising member of staff at the event), I agree not to share these pictures or videos on social media or online.

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.

I understand that my child must not bring personal electronic devices into school, and I will make sure that my child does not do this.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Name of School	**Nottingham Nursery School**
E safety policy review Date	**September 2020**
Date of next Review	**September 2023**

Acceptable Use: Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, , software, equipment and systems.

• I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

• I will not reveal my password(s) to anyone.

• I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.

• I will not engage in any online activity that may compromise my professional responsibilities, and I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Head teacher

• I will only use the approved, secure email system(s) for any school business. (This is currently: Office 365).

• I will not browse, download or send material that could be considered offensive to colleagues.

• I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

• I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.

• I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.

• I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

- I will embed the school's e-safety curriculum into my teaching.

- I understand that all Internet usage / and network usage can be logged and this information could be made available to my Head Teacher on request.

- I understand that failure to comply with this agreement could lead to disciplinary action.

Full Name .... (printed)

Job title ....

School Nottingham Nursery

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature .... Date ....

Full Name .... (printed)

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil or parent approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Do you keep your password for accessing the school's ICT systems secure and not share it with anyone else?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident