North Islington Nursery School & Children's Centre

ICT – Online Safety

Signed on behalf of Governing Body:

Date: August 2020
Review Date: August 2022

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 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 (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- 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 National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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).

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 headteacher

The headteacher 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 DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the School Business Manager, ICT manager 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 governing board

This list is not intended to be exhaustive.

3.4 The SBM & ICT manager

The school purchase a SLA agreement from the LA ICT department. The SBM will work alongside the ICT manager and 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
- 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)
- 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 they have read, understood 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 from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International

- Parent factsheet - Childnet International

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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4.1 Educating pupils about online safety

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

- Use technology safely and respectfully, keeping personal information private
- Practitioners will role model safe behaviour and privacy awareness. They will talk to the children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.

4.2 Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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

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

5. 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 1-3). 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, 2 and 3.

6. 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, they must seek advice from the SBM.

Work devices must be used solely for work activities.

7. 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.

8. 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. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

9. 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 every 2 years by the SBM. At every review, the policy will be shared with the governing board.

10. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: acceptable use agreement (parents/carers)

Acceptable Use Agreement: Parents/Carers

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They 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 Policy is intended to ensure:

- that young people 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 parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning. Due to the age of our children they are not able to sign an acceptable use policy.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form – Access to the internet

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that pupils will be safe when they use the internet and systems.

I understand that my son's/daughter's activity on the systems will be with adult supervision only.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed):	Printed
Who will have access to this form:	School staff
Where this form will be stored:	Child's file – lockable cabinet in Headteacher's office
How long this form will be stored for:	6 years after the child's leaving date
How this form will be destroyed:	Confidential shredding – external company 'Box It'

Pupil Name ……
Parent/Carers Name ……
Signed ……
Date ……

Permission Form – 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 the classroom.

Images may also be used to celebrate success through their publication in newsletters, on the school reception TV and occasionally in the public media. Where an image is publically shared by any means, the school will seek further permission from you.

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 in 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.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed):	Printed
Who will have access to this form:	School staff
Where this form will be stored:	Child's file – lockable cabinet in Headteacher's office
How long this form will be stored for:	6 years after the child's leaving date
How this form will be destroyed:	Confidential shredding – external company 'Box It'

As the parent/carer of the above pupil, I agree to the school taking digital/video images of my child — Yes / No

I agree to these images being used in the following ways:

- Internally – eg. Reception TV, display boards, within classrooms — Yes / No
- School monthly newsletter — Yes / No
- School website — Yes / No

- School prospectus and such publications such as promotional videos Yes/No
- I agree that if I take digital or video images at school events either on or off site which include images of children, other than my own, I will abide by these guidelines in my use of these images Yes / No

Pupil Name ……
Parent/Carers Name ……
Signed ……
Date ……

Permission Form – Use of Cloud Systems

The school uses Blossom Educational to track and record pupils learning and progress.

All parents/carers are sent a registration email to enable them to set up their individual log-in for the system, giving them access to their parent/carer page for their child's data only. (Please note that if your child is taking part in an activity with another child, this image may be shown on the other child's parent/carer page also – permission permitting)

Using Blossom Educational will enable school leaders to collate data and progress on all children at the setting. The system enables us to identify gaps in areas of learning and track their progress effectively. The room leader will make two observations per week parent-visible which enables you to log-in and see what your child has been doing whilst at nursery. These services are entirely online and available 24/7 from any Internet-connected computer, tablet or mobile using your unique parent/carer log-in for your child.

The school believes that use of the tools significantly enhances your child's educational experience. As the school is collecting personal data and sharing this with a third party, please be informed as follows:

This form (electronic or printed): Printed	*The data shared with the service provider:* Electronic
Who will have access to this form: School based staff	*What data will be shared:* Child details, contacts, observations, photos
Where this form will be stored: Child's file in locked cabinet in the Head Teacher's office	*Who the data will be shared with:* Only tech and support staff within Blossom Educational who have a need to know
How long this form will be stored for: 6 years after the child's leaving date	*Who will have access to the data:* Blossom Educational All staff employed by the school
How this form will be destroyed: Shredding – professional outside company	*Where the data will be stored:* Managed hosting service in Manchester
How the data will be destroyed: Deletion process performed by the tech manager	*How a request for deletion of the data can be made:* By request to the school, passed to tech manager

Do you consent to us having your child's data on Blossom Educational? ***(circle one)***	**Yes / No**

Pupil Name ……

Parent/Carers Name ……

Signed ……

Date ……

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

Acceptable Use Agreement: All Staff, Governors & Volunteers

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, software, communication tools, social networking tools, school website, equipment and systems.

North Islington Nursery School regularly reviews and updates all acceptable use agreement documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: Local Authority (LA)
- I will only use the approved email system, tracking system (My Nursery Child), SIMS and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Headteacher or SBM.
- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network 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 and other ICT 'defence' systems.

- I will not use personal digital cameras, camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

- I will follow the school's policy on the use of personal mobile phones / devices at school and will not take them into classrooms and only use in staff only areas or private meeting rooms.

- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the schools systems only.

- I will not take any school equipment home unless I have sought approval from the Headteacher.

- I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify pupils by full name, or other personal information.

- I will use the school's tracking system in accordance with school protocols.

- 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, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will only access school resources remotely (such as from home) using the school/LA approved system and follow e-security protocols to interact with them.

- 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 understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will alert the DSL/DDSL if I feel the behaviour of any child may be a cause for concern.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the DSL/DDSL.

- I understand that all internet and network traffic / usage can be logged and this information can be made available *to* the Headteacher/DSL on their request.

- I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

- I will only use any LA system I have access to in accordance with their policies.

- **Staff that have a teaching role only:** I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form
All Staff, Governors & Volunteers

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / child protection and safeguarding policies.

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

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Headteacher / SLT)

I approve this user to be set-up on the school systems relevant to their role.

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**:
Question	**Yes/No (add comments if necessary)**
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 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?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**