Online Safety Policy

1. Introduction

Young children are increasingly using technology and whilst the online world provides many opportunities, it can also present risks and challenges. Recent research found that 1% of 3-4-year olds have their own smartphone and 19% have their own tablet, 52% of 3-4-year olds go online for an average of nearly 9 hours a week and 45% of 3-4-year olds use YouTube. As children's access to technology increases, we recognise that our duty of care to keep children safe extends to the 'digital world' as well as the 'real world'.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff 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, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3. The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk for early years children:

Content (what they may see):

- Exposure to inappropriate videos. pictures or messages which might upset, worry or frighten them
- Imitating harmful or inappropriate behaviour they see online
- Searching for inappropriate content on purpose or stumbling upon it by accident. This would include using voice activated tools to search for content
- Inadvertently giving apps or websites permission to share their location or other personal information
- Spending real money via in-app or in-game purchases

Contact (who might communicate with them):

- Being abused online (including sexually) by people they don't know, such as when gaming or using video chat
- Being abused online (including sexually) by people they know, such as friends and family members
- Sending images or information to people on the device's contact list

Conduct (how they might behave):

- Exhibiting unhealthy behaviours and boundaries around their use of screens
- Being unkind to each other online as well as offline; this could be using mean words or by excluding others from their games
- Using words or terminology which are not appropriate for their age
- Engaging in unhealthy relationships
- As part of natural development, early years children may exhibit curiosity about their own and others' private body parts; if this occurs via technology children may be at risk of taking inappropriate or indecent images and videos of themselves

4. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE'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.

5. Roles and Responsibilities

5.1 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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss

with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

5.2 Head Teacher / DSL

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

As the DSL, the Headteacher will take lead responsibility for online safety in school, in particular:

- Review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Work with E-Services to make sure the appropriate systems and processes are in place
- Manage all online safety issues and incidents in line with the school's child protection policy
- Ensure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Update and deliver staff training on online safety
- Liaise with other agencies and/or external services if necessary

5.3 Technical Staff (Council E-Services/Corporate IT Dept)

Technical staff are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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
- Conducting a full security check and monitoring the school's ICT systems on an agreed timescale
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- This list is not intended to be exhaustive.

5.4 Staff

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 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

5.5 Parents/carers

Due to the age of our pupils, parents have a key role in keeping children safe online. Parents are important role models and the way they use technology can influence children's understanding of the acceptable use of ICT. Parents are asked to sign the schools 'Acceptable use of the internet: agreement for parents and carers' – appendix 2

Parents/carers 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 resource sheet – Childnet International

6. Educating pupils about online safety

We will teach children about online safety by:

- making them aware of what safe use of technology looks like
- choosing educational apps and platforms that help them to develop their skills
- having conversations and sharing advice with parents to encourage safe online use in the home

7. Educating parents/carers about online safety

We recognise that due to the age of our pupils they need support at school and at home to keep themselves safe. The school will communicate this policy to parents and share with them information about the systems the school uses to monitor and filter online use. The school will also raise parents/carers' awareness of internet safety at home and provide guidance and advice through a variety of communication channels including the welcome pack, letters and via the school web-site or app.

Parents will be encouraged to adopt the following guidance from the NSPCC for online safety for under fives:

- Set boundaries from the start. It makes it easier than trying to play catch-up at a later stage.
- Check that websites are suitable before your child visits them. Look for websites that have parental pages that explain how the site works and how they keep your child safe.
- Ensure your home page is set to a child-friendly website.
- Talk to friends about what websites their children use.
- Play games with your child to get them used to being online.
- Set 'Safety Mode' up on YouTube to help filter out explicit content.
- If you use Google, turn on Google 'Safe Search' to filter sexually explicit content from your search results.

8. Cyber-bullying

8.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power.

8.2 Preventing and addressing cyber-bullying

We recognise that due to the age and development level of our pupils the risk of cyberbullying is significantly lower than with other age ranges of pupils however we understand that where children have unsupervised access to technology there may be a risk to their safety.

The school will share information about cyber bullying with parents so that they are fully aware of the risks as their children grow and become more independent in their use of

technology. Information for parents/carers will include what signs to be aware of, how to report it and how they can support children who may be affected.

Through the curriculum staff will use teaching opportunities to develop children's personal and social skills and help them to understand the impact of their behaviour on others.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

8.3 Examining electronic devices

Children are not permitted to bring electronic devices into school however in the event that this occurs the headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

8.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Our Federation recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to bully pupils in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

9. Acceptable use of the internet in school

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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 staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in the appendices to this policy.

10. Pupils using mobile devices in school

Pupils are not permitted to bring mobile or electronic devices into school and this is communicated to parents/carers.

11. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 1.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

12. How the school will respond to issues of misuse

It is hoped that all members of the school community will be responsible users of digital technologies, however there may be times when infringements of the policy could take place, through careless or irresponsible, or very rarely, through deliberate 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. 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 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.

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

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every year by the headteacher.

15. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy

- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use of ICT policy

Policy reviewed November 2023.

Revised policy approved by the Full Governing Board on 10th November 2023

Bilston Nursery School

'Where children bloom and grow'
Eastfield Nursery School

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors and volunteers	
Name of staff member/governor/volunteer:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Email • My School App for parents (for school announcements, information about events, policy documents and photographs of the curriculum and activities that take place in school)	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns to the school directly, so that they can be dealt with in line with the school's complaints procedure I will not: • Use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Online safety incident report log

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