Online safety policy
Bispham Drive Junior School

Last reviewed on: October 2024
Next review due by: October 2025

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 to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:
Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism,misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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
Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
Relationships and sex education
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.
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 coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
The governor who oversees online safety is Cheryl Cooper (Chair of Governors)

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
Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

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 [Andrea Goetzee - Headteacher, David Belton - Deputy Head and Andrew Henshaw – SENCO, Linda Fitch - School Business Manager] are set out in our child protection and safeguarding policy as well as relevant job descriptions.
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, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
Managing all online safety issues and incidents in line with the school child protection policy.
Ensuring that any online safety incidents are logged (on the school safeguarding recording system, CPOMS) and dealt with appropriately in line with this policy.
Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy.
Updating and delivering staff training on online safety.
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 ICT manager

The ICT manager is responsible for:
Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 a fortnightly 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 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 (as recorded in the Acceptable Use Policy for School Laptops and Ipads), and ensuring that pupils follow the school's terms on acceptable use (as seen in pupils' Personal Organisers).
Working with the DSL to ensure that any online safety incidents are logged 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.

3.6 Parents

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (as seen in pupils' Personal Organisers).

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 resource sheet – Childnet International
Healthy relationships – Disrespect Nobody
Safer Schools App – Safer Schools App (Download Code for school: 4381)

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.

4. Educating pupils about online safety

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

National Curriculum computing programmes of study :
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.
It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

Relationships education and health education in primary schools

Pupils in Key Stage 2 will be taught to:

Use technology safely, respectfully and responsibly.
Recognise acceptable and unacceptable behaviour.
Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

That people sometimes behave differently online, including by pretending to be someone they are not.
That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
How information and data is shared and used online.
What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
The safe use of social media and the internet will also be covered in other subjects where relevant, especially through our termly topics.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. 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 or virtual learning environment (Google Classroom) 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 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. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
Where appropriate within the strands of the school Computing Curriculum (see Computing Overview on the Bispham Drive Website), the school will actively discuss cyber-bullying with pupils, explaining the

reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
The school also sends information/leaflets on cyber-bullying to parents and reminders through the school bulletin 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, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, 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*
* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.
Any searching of pupils will be carried out in line with:

The DfE's latest guidance on screening, searching 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.

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 (Acceptable Use Policy for School Laptops and Ipads/ (**Pupil Acceptable Use of Technology Agreement - Appendix A**).
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.

8. Pupils using mobile devices in school

Pupils may only bring mobile devices into school in exceptional circumstances if the parent has received permission from the headteacher In this case, children will not be allowed to use these during school hours.
Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (**Pupil Acceptable Use of Technology Agreement - see Appendix A**).
Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. 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).
Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
Making sure the device locks if left inactive for a period of time.
Not sharing the device among family or friends.
Installing anti-virus and anti-spyware software.
Keeping operating systems up to date – always install the latest updates.
Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in the 'Acceptable Use Policy for School Laptops and Ipads' policy.
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.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies listed on the school website . The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
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 code of conduct. 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).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Children can abuse their peers online through:

o Abusive, harassing, and misogynistic messages
o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
o Sharing of abusive images and pornography, to those who don't want to receive such content
Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

Develop better awareness to assist in spotting the signs and symptoms of online abuse.
Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.
The 4 DSLs 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in the school's internal safeguarding log system, CPOMS.
This policy will be reviewed every year by the Headteacher (Andrea Goetzee), School Business Manager (Linda Fitch) and Deputy Headteacher (David Belton). At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:
Child protection and safeguarding policy
Behaviour policy
Staff Code of Conduct
Data protection policy and privacy notices
Complaints procedure
ICT and internet acceptable use policy (to be found in pupils' Personal Organisers)
Acceptable Use Policy for School Laptops and Ipads (to be found in school office)
Pupil Acceptable Use of Technology Agreement (Appendix A).

Appendix A

Toton Bispham Drive Junior School

Ad esse optimum

Pupil Acceptable Use of Technology Agreement

At school we use computers, and other resources connected to the internet and our wireless network. These rules will keep us safe and help us to be fair to others:

• I will keep my passwords for login to any computer or application to myself and my adults at home – if I think others know my passwords I shall tell my teacher.
• I shall use the online activities and sites which school allows me to access from home appropriately.
• I will not bring in memory sticks into school unless I have been given permission.
• I will not use my own mobile device/ phone in school unless I am given permission from my teacher.
• If the computer asks for an update, I shall check this with my teacher.
• I will only use the computer for things my teacher has told me to.
• I will not use the internet to access unsuitable material.
• The messages I send will be polite and respectful.
• I will always report anything that I feel is unkind or makes me feel unsafe or uncomfortable to my teacher. I will not reply to any nasty messages.
• In school, I will only use websites my teacher has approved
• I will always keep my personal details private (e.g my name, mobile phone number, family information, journey to school, pets, hobbies).
• I will not register my details with online activities and websites without the permission of my teacher.
• I will not share files or photos without the permission of my teacher.
• I will not copy text or pictures from the internet and pretend it is my own work.
• I understand that the school will check my computer files and will monitor the Internet sites I visit.
• I will treat computer equipment, like all school equipment, with care and respect.
• I know that if I break the rules I might not be allowed to use a computer.

Signed _____