



Online safety policy

Last reviewed on:	October 2021
Next review due by:	October 2022

Contents

1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating parents about online safety	6
6. Cyber-bullying.....	6
7. Acceptable use of the internet in school	7
8. Pupils using mobile devices in school.....	7
9. Staff using work devices outside school.....	7
10. How the school will respond to issues of misuse.....	8
11. Training	9
12. Monitoring arrangements.....	9
13. Links with other policies	10
Appendix 1: online safety training needs – self audit for staff	11
Appendix 2: online safety incident report log.....	12

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 tablets and smart technology
- 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 Head Teachers 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 Head Teacher to account for its implementation.

The governing board will co-ordinate regular termly 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 Joan Walton.

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 (school Acceptable Use Policy).
- 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 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 DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions and are also available on the school website.

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

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Working with the Head Teacher, the Deputy, ICT Technician 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 and acceptable use policies.
- Ensuring that any online safety incidents are logged (see appendix 2) 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 anti-bullying policy.
- Updating and delivering staff training on online safety (appendix 1 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 Head Teacher and/or governing board.

This list is not intended to be exhaustive.

3.4 The ICT co-ordinator

As a school we have a Service Level Agreement with Entrust who provide the school with a designated ICT technician. Aspects of school's technical infrastructure and internet safety are delegated to the technician who is managed by the Deputy Head as the ICT co-ordinator. The ICT Technician and Deputy Head are 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 weekly basis.
- Ensuring that any online safety incidents are logged (see appendix 2) and reported promptly to the DSL who then ensures that any incidents of misuse and cyber-bullying are dealt with appropriately in line with the school anti-bullying and acceptable use 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 school's terms on acceptable use with regards to the school ICT systems/ facilities and the internet and ensuring that pupils also follow the school's terms.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 2) and dealt with appropriately.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school anti-bullying 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 Head Teacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the specified terms on acceptable use of the school's ICT systems and internet.

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](#)

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 school's terms on acceptable use.

4. Educating pupils about online safety

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

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All primary schools have to teach: [Relationships education and health education](#)

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

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.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

In school we also have E-safety and school councils, who promote acceptable use and safety guidance across the school through varied activities such as engaging the children in signing E-safety contracts, delivering assemblies and participating in themed safety days/ weeks. These measures further support us as a school, to protect and educate pupils, and all of our staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

5. Educating parents about online safety.

The school will raise parents' awareness of internet safety through letters, via the school Facebook page, text or emails home, and in information via our website. This policy will also be shared with parents.

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

Concerns or queries about this policy can be raised with the Head Teacher.

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 anti-bullying 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.

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.

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 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 anti-bullying 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 and or the Head Teacher 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.

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. 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, 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 school acceptable use policy.

8. Pupils using mobile devices in school

Pupils are not permitted to have mobile/ electronic devices in school. Any electronic device found in school will be safely retained by the teacher, sent to the office or sent to SLT until the end of the day for collection by the parent or carer.

9. Staff using work devices outside school

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

- Only being able to access the device by logging on with their individual school username and being personally responsible for setting secure passwords. Strong passwords should be at least 8 characters, with a combination of upper and lower-case letters and numbers.
- Ensuring that data needing to be kept securely is on the provided password protected memory stick - this means if the device is lost or stolen, no one can access the files stored on it by attaching it to a new device.

- Making sure the device is locked if it will be left inactive for a period of time.
- Not sharing the device among family or friends.
- Not leaving devices unattended in vehicles.

Staff members must not use the device in any way which would violate the school's terms use, as set out in the acceptable use policy.

If staff have any concerns over the security of their device, they must seek advice from the Deputy Head Teacher or DSL or another member of the Senior Leadership Team.

We allow staff to access the school's ICT facilities and materials remotely.

Teaching staff can access the schools' server and saved resources via the internet remotely. Any teacher may use their personal login to access through a website called Foldr. Teachers may access the server with the same level of clearance that they have when in school. Files can be worked on and saved onto the server without needing to download them. Files may be retrieved and saved locally but these should not contain personal data unless they are encrypted or saved to the school laptop/ memory sticks provided. New files can also be created and saved to the server avoiding the need to transfer files on portable memory sticks.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site.

10. How the school will respond to issues of misuse

It is more likely that that school may need to deal with incidents of inappropriate use rather than incidents of illegal misuse. Where a pupil misuses the school's ICT systems or internet, we will deal with the incident as soon as possible and ensure that all members of the school community are made aware of the actions which are taken. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Incidents will be dealt with through normal behaviour/ disciplinary procedures examples of which include;

- Referral to the class teacher,
- Receiving a warning/ movement down the behaviour board and future monitoring,
- Parents/ carers informed,
- Work removed/ deleted from the system,
- Loss of free time e.g. play times,
- Additional work on remaining safe online with individual/ class/ school - as deemed appropriate.
- Access to the school ICT facilities will be removed,
- Incidents will be logged,
- ICT technician will be prompted to check the filtering and security systems,
- Referral to the Senior Leadership Team/ Head Teacher where incidents are more severe or are not the first occurrence,

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 by the Head Teacher. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident and will be in line with disciplinary action.

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

Incidents to report would include;

- Inappropriate/ obscene images of children,
- 'Grooming' behaviours,
- Adult material
- Racist material,
- Promotion of terrorism or extremism
- Links to other criminal activity

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:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- 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 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.

Further 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 2.

This policy will be reviewed every year by the DSL. The review will include the completion of a whole school audit and 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. Following every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

Safeguarding and Child protection policy

Anti-bullying policy

Staff handbook including staff code of conduct

Data protection policy and privacy notices

Complaints procedure

Acceptable use internet access policy

Safe and appropriate use of images in schools and settings

Appendix 1: 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?	
Are you aware of the ways pupils can abuse their peers online?	
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? Does your password contain upper and lower case letters and numbers?	
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?	

Appendix 2: online safety incident report log

[illegible]