Online Safety Policy

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

> 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:

1. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism Students may be accessing age-inappropriate or unreliable content. Some online content is not suitable for students and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It is important for students to consider the reliability of online material and be aware that it might not be true or written with a bias. Students may need our help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

2. **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
Students can be contacted by bullies or people who groom or seek to abuse them. It is important for students to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, they may be sharing their personal information with them. Regularly reviewing friends' lists and removing unwanted contacts is a useful step. Privacy settings online may also allow them to customise the information that each friend is able to access. If a student is, or has been, the subject of inappropriate sexual contact or approach by another person, it should be reported to the police. Students should know how to report it online via the Child Exploitation and Online Protection Centre (www.ceop.police.uk) and need to know the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online. If a student is the victim of cyberbullying, this can also be reported online and offline.

3. **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.
Students may be at risk because of their own behaviour, for example, by sharing too much information. They need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It is easy to feel anonymous online and it's important that students are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it is important to keep personal information safe and not share it with strangers. Students should know the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done.

4. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

   Students can be unaware of hidden costs and advertising in apps, games and websites. Their privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Students should be encouraged to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms. The 4 Cs do not stand in isolation, however, and it is important to understand the interplay between all four. For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming or images (formerly known as 'sexting').

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 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 3)

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:

> 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

> Ensuring that any online safety incidents are logged (see appendix 5) 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 4 contains a self-audit for staff on online safety training needs)

> Liaising with other agencies and/or external services if necessary

> Providing regular reports on online safety in school to the headteacher and/or governing

board   This list is not intended to be exhaustive.

3.4 The ICT Lead

The ICT manager 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

> Conducting a full security check and monitoring the school's ICT systems on a weekly basis

> Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

> Ensuring that any online safety incidents are logged (see appendix 5) 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

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

> Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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

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 (appendices 1 and 2)

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 3).

4. Educating pupils about online safety

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

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*

> *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.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also
invite speakers to talk to pupils about this.

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. 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.

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, and the issue will be addressed in assemblies.

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 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

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

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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.

8. Pupils using mobile devices in school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

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 3.

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 ICT

manager. Work devices must be used solely for work activities.

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 on   behaviour and ICT and internet acceptable use. 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 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).

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 appendix 5.

This policy will be reviewed every year by the IT Lead. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

> Child protection and safeguarding

policy > Behaviour policy

> Staff disciplinary procedures

> Data protection policy and privacy

notices > Complaints procedure

> ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:
I will read and follow the rules in the acceptable use agreement policy   **When I use the school's ICT systems (like computers) and get onto the internet in school I will:**   • Always use the school's ICT systems and the internet responsibly and for educational purposes only   • Only use them when a teacher is present, or with a teacher's permission   • Keep my username and passwords safe and not share these with others   • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer   • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others   • Always log off or shut down a computer when I'm finished working on it   **I will not:**   • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity   • Open any attachments in emails, or follow any links in emails, without first checking with a teacher   • Use any inappropriate language when communicating online, including in emails   • Log in to the school's network using someone else's details   • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision   **If I bring a personal mobile phone or other personal electronic device into school:**   • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a   teacher's permission   • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online   **I agree that the school will monitor the websites I visit and that there will be consequences if I don't**

Signed (pupil):	Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	Date:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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 • Take photographs of pupils without checking with teachers first • 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 will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree 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) and ICT manager 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.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: 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 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 5: 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