Online Safety and ICT Procedures Policy

Approved by:	Full governing body	**Date:**	11th March 2024
Previously reviewed on:	Autumn 2023		
Next review due by:	Spring 2025		

Chair of governor's signature

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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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 body

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

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

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The headteacher

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

The Headteacher is responsible for ensuring that staff are adequately inducted and trained by users, and that support is provided to enable them to implement the policy.

The Headteacher is responsible for equipment disposal in accordance with Electrical and Electronic Equipment Directive (WEEE)

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection/safeguarding policy.

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 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the 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 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. This will be in line with Keeping Children Safe in Education, September 2023.
- 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 (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Data protection. All users are expected to act in a lawful, ethical and responsible manner. Users should uphold privacy and confidentially in accordance with the data protection act 2018. http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted This includes taking appropriate measures to secure data during working process, in transit or when in storage.

This list is not intended to be exhaustive. Violations of this policy or failure to implement this policy might lead to an immediate suspension of an individual's permission to access the school network, followed by an investigation and/or disciplinary procedures. If an individual suspects that a pupil, member of staff or visitor has violated the policy, they should contact the Headteacher in the first instance. If the headteacher's conduct is brought into question, the chair of governors should be contacted.

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 (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. 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

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. 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 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 and 2). 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.

Inappropriate content is defined as, but not limited to:

- Pornographic material
- Gratuitous violence, injury or death images
- Material that is likely to lead to harassment of others
- Material that promotes intolerance and discrimination on the grounds of race, sex, disability, sexual orientation, religion, belief or age.
- Material relating to criminal or unlawful activity
- Material that might generate security risks or encourage computer misuse

It is possible to access or be directed to unacceptable sites by accident. This can be embarrassing and such sites can be difficult to get out of. If users have accessed unacceptable content or are in receipt of it via email they should inform the Headteacher.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils **may not** bring mobile devices into school unless prior permission has been obtained from a member of the SLT or a DSL. In this instance, the pupil's mobile device must be held securely by a member of SLT or a DSL.

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 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the 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 the behaviour policy. 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

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).

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.

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 4.

This policy will be reviewed annually by the Online Safety Committee. At every review, the policy will be shared with the governing body.

13. Links with other policies

This online safety policy is linked to the following policies

- Child Protection and Safeguarding policy
- Behaviour policy
- Information Management Handbook
- Complaints procedure
- SEN Policy

14. Bring Your Own Devices (BYOD) and Personal Use of Devices

A BYOD includes, but is not restricted to, phones, tablets, laptops, smart watches, ipods and MP3 player. The school does not advocate the use of using personal devices as part of pupil's learning.

The school allows the following:

	SCHOOL DEVICE		PERSONAL DEVICE			
	School user with individual log-in and password	Multi-user, such as a supply teacher	Staff owned	Pupil owned	Visitor (on school business) owned	Parents
Allowed in school	Yes	Yes	Yes*1	No, unless permission given by a member of SLT or DSL. Device then to be stored safety by SLT or DSL.	Yes*1	Yes and no*2
Access to WIFI/Internet	Yes	Yes	Yes, if AUA is signed.	No	Yes, if AUA is signed.	No
Access to network	Yes	No	No	No	No	No

*1: Staff and visitors on school business are allowed to use personal devices in school, but they should not carry out personal matters (i.e calls/messages) in the presence of pupils. Where possible, personal matters should be dealt with outside of teaching time, and in a room with the door closed. Staff and visitors on school business should not use personal devices under any circumstances to photograph or record pupils.

*2: When an event is organised by the school, and held in school hours, such as open mornings, reading cafes etc, parents must not use their own mobile devices whilst in school.

When an event is organised by an outside body, e.g the PTA, and is to be held outside of school hours, e.g. Easter egg hunts, Christmas Fairs etc parents are allowed to use their own mobile devices, but they should not take photographs or record other people's children without explicit permission from a legal guardian. Photographs of other people's children should not be shared on social media with permission of the child's legal guardian.

Email and school work on personal devices

Staff may use their personal devices to access school-related emails. Staff must ensure that their personal 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 personal device if emails are accessed on it. Any USB devices containing data relating to the school must be encrypted or password protected.

Email, personal business and school work on school devices

In the course of normal operations ICT resources are to be used for school purposes. The school permits the personal use of ICT facilities for things such as online banking and word processing for personal use by authorised users, subject to the following limitations:

- Must be in the user's own time and must not impact upon the school efficiency or costs.
- Must be reasonable level of use and not detrimental to the main purpose for which the facilities are provided
- Must not be of a commercial or profit making nature
- Must not be of a nature that competes with the business of the school or conflicts with an employee's obligations
- Must not conflict with any aspect of this policy
- Must not use the school email address to register for access to websites for personal use, e.g online shopping.

15. Use of Social Networking

Personal use of the internet

The school restricts and monitors access to social networking websites from its computers at all times. Access will normally only be allowed where use of such websites is for school purposes.

Personal Conduct

The school respects staff's right to a private life. However, the school must also ensure that confidentiality with regards to it pupils, employees, visitors and volunteers and its reputation are protected. Therefore, the school requires staff and governors using social networking websites to:

- Use caution and act responsibly when posting information
- Refrain from identifying themselves as being connected to the school
- Ensure that they conduct themselves in a way that does not conflict with their professional code of conduct or in a manner that is detrimental to the school. This includes, but is not limited to, online harassment'bullying, and using defamatory statements

The headteacher should be notified of any misconduct with screenshots of the inappropriate content. The school takes seriously such incidents and the matter will be investigated, which could lead to disciplinary procedures.

Staff must not be 'friends' or communicate with pupils via social networking. If a pupil makes contact with a member of staff (or another individual associated with the school), the headteacher should be notified as soon as possible. In the headteacher's absence, a member of the senior leadership team should be notified. The school takes seriously such incidents and the matter will be investigated, which could lead to disciplinary procedures.

16. Passwords

All staff must have a unique user name and password. The password should be distinct and different from their user name. Strong passwords are recommended. Staff must not:

- Share their passwords with anybody at all.
- Insert their passwords into any electronic communication such as email
- Log onto a machine using their user name and password for another user to use.
- Keep their password for a prolonged amount of time. It should be changed regularly.
- Use 'remember password' feature on websites which contain school data

If a member of staff feels that their password has been compromised, they should contact the headteacher who will contact the IT technician and consider reporting a data breach.

Pupils in KS2 should have unique passwords to log on to the school's network. The passwords should be kept securely and must not be shared with other pupils. School staff will keep a log of pupil passwords. Pupils should change their passwords annually.

17. Images of pupils and staff

The word 'image' includes photographs, digital photographs, webcam, film and video recordings. The school will only use images that the headteacher and governing body consider suitable and which appropriately represent the range of activities in school, whilst adhering to the school's ethos, values, and safeguarding procedures.

Data protection

Images of pupils and staff are classed as personal data under the terms of the Freedom of Information act 2000. We will not use images that identify individuals without the consent of the individual, or in the case of pupils, their parent/guardian. A consent form for children is required when they enroll into the school.

All images will be stored only on school devices and by those authorized to store such items.

Staff are not permitted to take photographs or recordings of children on personal devices without explicit permission from the headteacher. In such cases, the images are not permitted to be removed from the school site without permission from the headteacher.

18. Email

Staff are asked to consider email etiquette before sending emails:

- Consider an alternative such as a face-to-face conversation
- Keep emails to a minimum and do not copy people in unnecessarily
- Use professional and clear language, and do not mix personal and business matters
- Give emails a meaningful title
- Only request read receipts if necessary, not as default.
- Do not forward personal messages or material that will breach copywrite without permission
- Do not send unnecessary very large files which will take up room in the recipient's email account
- Do not email after 5:30pm and at weekends unless absolutely necessary
- Use the 'delay send' function to minimise out of hours emails.

Staff must not email pupils unless it is about a school matter. Such emails must always be sent from the staff member's school email account.

Staff and pupils must not:

- Use a false identity in emails or create anonymous messages
- Create or alter an email with the intention of deceiving the recipient.
- Create, transmit or forward illegal, offensive or indecent material or material that will cause anxiety or annoyance to the recipient.

Personal data

Staff must not transfer sensitive personal data via email. Sensitive personal data is defined as:

- Racial or ethnic origin
- Political beliefs
- Religious beliefs (or other beliefs of a similar nature)
- Membership of a trade union
- Physical or mental health condition
- Sexual life
- Criminal convictions

When referring to a pupil in emails, first names (or initials) only must be used.

Emails will be checked if:

- There is reasonable cause to believe the member of staff or pupil has violated or violating this policy
- An account appears to be engaged in unusual or excessive activity
- It is necessary to protect the integrity, security or functionality of ICT resources or to protect the school from liability.
- Establishing the existence of facts relevant to school business
- Preventing or detecting crime
- Investigating or detecting unauthorised use of email facilities
- Determining if emails are related to school business (for example if a member of staff is off sick or on holiday) as a last resort.

All monitoring will be carried out in accordance with the Information Commissioner's Office (ICO) code of best practice on monitoring employees.

Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the 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, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details • Leave the device unlocked when not under direct supervision	
I agree that the school will monitor the websites I visit. 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. This includes not leaving a school device in an unattended vehicle. 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. 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:**

Appendix 2: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
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? Please record them here.	

Appendix 3: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**