Online safety policy

Castledon School

Approved by:	FGB	**Date:**	28th March 2023
Last reviewed on:	March 2023		
Next review due by:	March 2024		

Contents

1. Aims

2. Legislation and guidance

3. Roles and responsibilities

4. Educating pupils about online safety

5. Educating parents about online safety

6. Cyber-bullying

7 Pupils using mobile devices in school

8. Use of social media

9. Staff using work devices outside school

10. How the school will respond to issues of misuse

11. Training

12. Monitoring arrangements

13. Links with other policies

Appendix 1: Internet Safety Curriculum

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, antisemitism, 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 scams

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- 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.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trustee board

The trustees have 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).

The Trustee responsible for Safeguarding who oversees online safety

All Trustees will:

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

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 designated safeguarding lead (DSL) deputies 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 (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 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
- Work with external providers to ensure security checks and monitoring takes place on the school's ICT systems
- 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 and Relatioships 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 of use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms of use
- Working with the DSL to ensure that any online safety incidents are loggedand 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 and Relationships 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'

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

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

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.

4. Educating pupils about online safety

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

Online safety is taught in ICT and lessons and in RSHE.

Each Key Stage follows its own curriculum map. Please see the appendices for further information.

https://docs.google.com/document/d/10ON118RhAYJTr0rr_WOI8J2E5B096wCo/edit

RSHE curriculum https://docs.google.com/document/d/1402PGi4573yC6P2uwIcIR4tFJzZG8qKl/edit

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
- Relationships and sex education and health education in secondary schools

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.

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 and social media.

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 Designated Safeguard Lead (DSL) or Deputy Desingated Safeguard Leads (DDSL).

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

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/form teachers will discuss cyber-bullying with their classes/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, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher and SLT, and, with the headteacher's authorisation, other members of staff, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

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

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

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

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

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

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

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

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

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

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour and relationships policy
- 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. Pupils using mobile devices in school

KS1-4 pupils may bring mobile devices into school for use on transport but are expected to hand them in where they are put in a lockable box.

KS5 students are permitted to mobile devices in to school but are not permitted to use them during:

- Lessons (unless given permission by teaching staff)
- Tutor group time (unless given permission by teaching staff)

- Clubs before or after school, or any other activities organised by the school including residentials (unless given permission by teaching staff)

8. Use of social media

Social media and social networking is often essential to young people's lives – it's how they keep in touch and communicate with friends, family and schoolmates.

Personal mobile devices mean that children and young people can be active on social media anywhere and at any time. This can provide new opportunities for children and young people to learn and express themselves. But it can also present risks, including:

- cyberbullying
- online grooming
- emotional abuse
- online abuse.

As a part of children and young people's day-to-day safety, these issues are addressed in the classroom and as part of an open, ongoing conversation about online safety, so that our pupils can learn about how to stay safe on social media. Any misuse will be responded to in line with our Behaviour and Relatonships Policy

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
- Keeping operating systems up to date by always installing the latest updates (including anti-virus and anti-spyware software where necessary)

Staff members must not use the device in any way which would violate the school's Code of Conduct

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 ICT Manager.

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 Behavior and Relationships 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/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.

10. Training

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 up the risks
- 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 Level 3 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.

Trustees 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.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on the school's electronic recording system (CPOMS).

This policy will be reviewed every year by the Head of ICT with RSHE Leads and DSL.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and Relationships Policy
- Staff Code of Conduct
- Bring Your Own Device Policy
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Internet safety curriculum

Castledon School ICT Curriculum Overview

YEARS 1 - 4		Year 1 2019-2020	Year 2	Year 3
Autumn	First	Recognising personal information, knowing what adults can help me when using technology and following instructions when using a computer.	Understanding that not everything is real on the internet and how to ask an adult for help	Understanding how to use computers and technology safely
	Second	Naming parts of a computer and mouse/touchpad skills	To recognise how technology is used in different places (home, school, community)	Knowing adults who can help me and making safe choices when using technology
Spring	First	Using a keyboard	Digital painting using mouse and touchpad skills	Retreieving information from the internet (using Purple Mash)
	Second	To create content using touchpad, mouse and typing skills	To manipulate content using a touch, mouse and typing skills	To create content using information from the internet
Summer	First	Using computer programmes (understanding that computers need precise instructions)	Making predictions using coding	Creating a coding programme
	Second	Recognising the differences between online experiences and experiences not using the internet. Using the internet safely and recognising the reasons for safety	Being a good friend and making safe choices when using computers	Making safe choices when using a computer

		rules when playing games and watching videos online.		

YEARS 5-6		**Year 1**	**Year 2**
Autumn	First	Using computers safely and recognising parts of a computer (input and output devices)	Recognising trusted adults, how to ask for help and how to be safe when sharing information.
	Second	Using a touchpad and mousepad to click and drag, scroll and make choices	Understanding how people use computers and technology
Spring	First	Using a keyboard (using both hands to type, typing numbers and a basic sentence)	Collecting information using computers, including online communication
	Second	Sequencing computer programmes using coding skills	Solving problems using coding
Summer	First	Using a search engine, understanding how a results page works and where to find information	Online research using the internet
	Second	Online safety when sharing information	Knowing the difference between online and offline experiences (friendships with people, recognsing risks online)

YEARS 7 - 9		Year 1	Year 2	Year 3
Autumn	First	Protecting our online identity and identifying different ways that people choose to represent themselves online (including recognising when an unsafe link or website is asking for personal information)	Cyberbullying and healthy online relationships (offline vs online behaviours)	Recognisng unsafe behaviours online, how to avoid online conflict and how to report concerns
	Second	Trusting online sources (including body image, content and recognising when information is targeted)	Using a search engine and recognising trusted online resources	Understanding hardware and software
Spring	First	Typing, editing and formatting a document	Creating a presentation (including plagiarism and copyright)	Collecting information from people and presenting information to others (speadsheet, graphs)
	Second	Understanding how the internet works and what a network is	Collecting information using the internet and presenting information to others (collecting information using a search engine and trusted websites, presenting information using Google slides)	Editing and formatting skills (using templates)

Summer	First	Understanding what consent means when sending photographs, online messages, streaming and videos	Computer programming languages	Solving programs and creating coding programmes
	Second	Planning tasks using computers (using maps, finding information online, recording information)	Online communication (including unsafe messaging, stranger danger)	Identifying postive and negative ways that people use the internet and what to do if you see something unsafe online (including age restrictions)