Orion Coopers

Policy Name: Online Safety

Policy Date: September 2026
Renewal Date: September 2027
Author: K Choudhury
Owner: Assistant Headteacher, Personal Development

Type of Policy:

☐ Trust Policy

☒ Trust policy tailored by School

☐ School Policy

Approval:

☒ School

☐ LAB

☐ Board

020 8467 3263
orioncoopers.org.uk
info@orioncoopers.org.uk

Orion Coopers
Hawkwood Lane,
Chislehurst,
Kent BR7 5PS

Orion Coopers

Our Four Critical Questions

Why do we exist?

To improve outcomes, transform lives and enable social mobility.

How do we behave?

Trust • Kindness • Endeavour

What do we do?

We create a strong network of schools which transform the lives of students by enabling them to achieve high educational and personal goals, regardless of their background.

How do we succeed?

Through a clear backbone, strong culture, academic rigour and smart systems.

Contents

1. Policy Statement..... 4
2. Aims 4
3. Legislation and guidance..... 4
4. Roles and responsibilities 5
5. Educating and Curriculum 6
6. Educating parents about online safety.....7
7. Cyber-bullying 7
8. Acceptable use of the Internet in school.....9
9. Pupils using mobile devices in school.....9
10. Staff using work devices outside school 9
11. How the school will respond to issues of misuse 10
12. Training..... 10
13. Policy Review..... 10

Appendix 1: Student IT Policy and Acceptable use agreement (pupils and parents/carers) 11

1. Policy Statement

This policy outlines our commitment to safeguarding all members of the school community in their use of digital technologies. It applies to all staff, pupils, governors, volunteers, parents/carers, and visitors who access school systems or use personal devices on school premises.

2. Aims

Our school aims to:

- Protect pupils, staff, volunteers and governors from online harm.
- Promote responsible and respectful digital behaviour for the whole school community, including mobile and smart technology e.g. mobile phones.
- Embed online safety across the curriculum and school culture.
- Provide clear procedures for responding to online safety incidents.

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-nude and/or pornography), sharing other explicit images and online bullying

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

3. 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, sex and health 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.

4. Roles and responsibilities

a) The Local Advisory Board

The LAB has overall responsibility for monitoring this policy and holding the Principal to account for its implementation. The governing board will coordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

b) The Principal

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

c) The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection policy as well as relevant job descriptions.

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

- Overseeing online safety and dealing with any safeguarding concerns that are reported in relation to online safety.
- 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 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 as part of Safeguarding training.
- Liaising with other agencies and/or external services if necessary

d) The ICT manager/Trust IT support

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 regularly to assess the 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
- 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

e) 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, and ensuring that pupils follow the school's terms on acceptable use
- Reporting any concerns to the DLS or SLT for Behaviour.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

f) 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
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
  What are the issues? - UK Safer Internet Centre
  Help & advice | Childnet
  Parents and Carers resource sheet | Childnet

5. Education and Curriculum

Pupils will be taught about online safety as part of the curriculum.
Online safety is taught through:

- IT and Computing lessons
- PSHE Curriculum (including RSHE)
- Assemblies and Tutor time Curriculum
- Any other appropriate resources

Topics covered include:

- Cyberbullying
- Online grooming and exploitation
- Sharing of nudes/semi-nudes
- Misinformation/disinformation
- AI and emerging risks

Pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

6. 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 other information events.

This policy will also be available to parents.

If parents have any queries or concerns about 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.

7. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps, gaming sites or online conversations whilst gaming.

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. (See also the school behaviour policy.)

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. 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.

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.

Examining electronic devices

Any member of staff may carry out a search and confiscate any electronic device if they have reasonable grounds to suspect that the device may contain material or be used in a way that breaches school policy or poses a safeguarding concern.

This may include material that:

- 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 the staff member will:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff.
- 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 DSL, Principal, or 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.

Images of a sexual nature should not be looked at and an appropriate response, including notifying external agencies as appropriate, will be put in place.

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 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 immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance:
  Searching, screening and confiscation in schools - GOV.UK
  Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK

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

8. Acceptable use of the Internet in school

All pupils, staff, and volunteers 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 of acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or to fulfil 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.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school but these are put into Yondr pouches at the start of the day and unlocked as pupils leave. 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.

10. Staff using work devices outside of 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.
- 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
- Staff members must not use the device in any way which would violate the school's terms of acceptable use.
- 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.

11. How the school will respond to misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our 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 and 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.

12. 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, staff bulletins and staff meetings).

Training will 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 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.

13. Policy Review

This policy will be reviewed annually or following any significant incidents or changes in guidance. Input from staff, parents and pupils is encouraged where applicable.

Appendix 1- Student User Policy

This Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Rules for Responsible ICT Use

These rules will also be displayed every time you log on to a computer and you must digitally agree to the rules before you are allowed to logon to the School ICT network.

Orion Coopers School does not permit the following activities:

- Sending or displaying offensive messages or images
- Accessing undesirable material e.g. pornography
- Accessing social networking sites/chat rooms during lessons
- Listening to music or playing games from websites whilst learning
- Posting undesirable messages on a website or the Learning Gateway
- Knowingly introducing viruses onto the school network
- Using another users password
- Accessing another users files and folders
- Intentionally wasting resources used for printing
- Students should not contact staff through any social networking platform other than the Orion Coopers School email
- Using racist, sexist, homophobic, violent or abusive language during the conduct of emails or other Internet activities
- Interfering with the functioning of the school network or any other network that can be accessed via the Internet

For security purposes your actions and files will be monitored remotely and your actions recorded.

In cases of vandalism we will seek reimbursement from the perpetrator(s) to cover the cost of repair or replacement.

Secure Password Protection:
In order for passwords to be secure you must:

- Avoid choosing obvious passwords (such as your names, date of birth etc.)
- Not to choose common password (such as password, 12345, coopers etc.)
- Not write down your password. If you have too many passwords to memorize, record them in a computer file then encrypt the file with password protected. You must memorize this password and do not record anywhere.

The system will:

1. Enforce password history – 4 passwords remembered
   (When changing password, you cannot use last 4 remembered passwords)
2. Maximum password age – 365 days
   (You are now enforced to change your password every 12 months)
3. Minimum password age – 0 days
   (You can change your password anytime you wish)
4. Minimum password length – 8 Characters
5. Password must meet complexity requirement – Enabled

   Your password must contain characters from three of the following four categories:
   - English uppercase characters (A through Z)
   - English lowercase characters (a through z)
   - Base 10 digits (0 through 9)
   - Non-alphabetic characters (for example, $, #, %)

6. Account lockout duration – 5 minutes
7. Account lockout threshold – 8 invalid logon attempts
   If you failed to logon with 8 invalid password attempts, your account will be locked out.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents/carers, exclusion and in the event of illegal activities involvement of the police

ICT ACCEPTABLE USE AGREEMENT FORM – HOME COPY

Student name: _____ Date of Birth: _____/_____/_____

Parent Section

As the parent or carer of the above student(s), I grant permission for my child(ren) to have access to use the Internet, school e-mail and other ICT facilities at school.
I know that my child(ren) has read, understood and agrees to abide by the ICT Users Policy and has signed this ICT Acceptable Use Agreement.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the School will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching e-safety skills to students.

I understand I will be provided with a username and password to access the parent portal. It is my responsibly to keep this password safe in order to prevent unauthorised access to my child's information. I will contact the school immediately if I suspect my password has been compromised.

I understand that the school can check my child's computer files, and the Internet sites they visit and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / Carer name: _____

Parent / Carer signature: _____ Date: ____/_____/_____

Student Section

I have read, understood and agree to the rules included in the ICT Student Users Policy and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, google classroom, website etc.

Student name: _____

Student signature: _____ Date: ____/_____/_____

If you do not sign and return this agreement, access will not be granted to school ICT network and system.