CITY OF ROCHESTER SCHOOL

ONLINE SAFETY POLICY

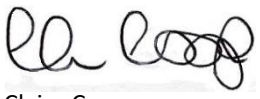
This policy, which applies to the whole school, and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office. This policy is also publicly available on the school website

Monitoring and Review:

- This policy will be subject to continuous monitoring, refinement and audit by the Headteacher, being responsible for the day to day organisation of the curriculum, monitoring the weekly lesson plans for all staff, ensuring all planning is appropriately differentiated with relevant, appropriate learning objectives.
- The Headteacher along with the whole school teaching and therapy team review the long-term and medium-term planning and ensure that appropriate targets and strategies are in place. It is intended that the ongoing review and development of the curriculum will support enthusiastic and inspirational teaching. The process of review plays a key role in the continuing professional development of all staff at City of Rochester School.
- The Trustees undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so requires. This discussion will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay.

Signed:

Date Reviewed: September 2021
Date of Next Review: September 2022
Version No. 3
Policy No 19b:001



Alicja Emmett
Headteacher

Claire Cooper
Chair of Trustees and Safeguarding Trustee

This policy will be reviewed no later than September 2022, or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.

Table of Contents

1. Introduction

1.1 Background: At City of Rochester School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for young people and play an important role in their everyday **lives. Whilst City of Rochester School recognises the importance of promoting the use of computer technology throughout its activities and curriculum, we also understand the need for safe internet access and appropriate use. City of Rochester School has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all young persons and staff.**

City of Rochester School is committed to providing a safe playing, learning and teaching environment for all young people and staff, and has implemented important controls to prevent any harmful risks. To be read alongside:

- Social media policy
- Safeguarding policy
- Anti-bullying policy
- Prevent policy

1.2 Use of the internet: City of Rochester School understands that using the internet is important when raising educational standards, promoting achievement and enhancing teaching and learning. Internet use is embedded in the statutory curriculum and is therefore an element for all young persons, though there are a number of controls City of Rochester School is required to implement to minimise harmful risks.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- 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

1.3 Online Safety

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2 Roles and Responsibilities:

2.1: The trustees: The trustees have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The trustees 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 trustees 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

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

2.2: Online Safety Officer: Michelle Homer (Deputy Headteacher) is the Online Safety Officer for City of Rochester school. It is her responsibility for ensuring the day-to-day e-safety in City of Rochester School's buildings and activities, managing any issues that may arise. The Online Safety officer will provide relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach young people about online safety. All staff complete National Online Safety Certified training as part of their induction. The Online Safety Officer will regularly monitor the provision of online safety within City of Rochester School and will provide feedback to the Headteacher. All staff have a CPOMs log in to log any incidents and inappropriate internet use, either by pupils or staff. The Online Safety Officer ensures that all relevant members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded. Please see the employee handbook for further information on monitoring. The Online Safety Officer is responsible for communicating with parents and regularly updating them on current online safety issues and control measures.

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

2.4 The designated safeguarding lead: Details of the school's DSL and DDSL's 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 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or trustees

This list is not intended to be exhaustive.

2.5 The Business manager and ICT manager: The business manager and ICT manager are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly 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 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.

2.6 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
- Working with the DSL to ensure 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 policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

2.7 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
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

2.8 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.

3 Online Safety Education

3.1. Educating Young People and Students: An online safety programme is established and taught through Computing, PSHE and RSE and delivered to young people in an age appropriate manner so that all develop an awareness of how to use the internet safely both inside and outside of City of Rochester School. Young people will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content. Young people will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism. Clear guidance on the rules of internet use will be displayed in classrooms. Young people will be made aware as to how to report any inappropriate use of the internet and digital devices and be told that it is their responsibility to do so. City of Rochester School will use I Need To Talk slips so young people can make anonymous reports should they find this necessary. The taught curriculum for the educational aspects of City of Rochester School will be used to educate pupils about cyber bullying, including how to repot cyber bullying, the social effects of spending too much time online and where to access help. City of Rochester School will hold such online safety events as are necessary and appropriate in order to promote online safety effectively. Such as Safer Internet Day and Anti Bullying Week.

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

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, 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

Pupils in **Key Stage 4** will be taught:

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

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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.

3.2 Educating Staff: A planned calendar programme of online safety training opportunities will be available to all staff members, including whole charity activities and CPD training courses. All staff will undergo online safety training annually/when changes occur basis to ensure they are aware of current online safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole. All staff will employ methods of good practice and act as role models for young people when using the internet and other digital devices. Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this online safety policy/social media policy/user agreement.

3.3 Educating Parents: The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our Facebook page. Parents are also given access to National Online Safety Training. 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.

4 Online Safety Control Measures

4.1 Internet Access:

- Internet access will be authorised once parents and young people have returned the signed consent form in line with our Acceptable Use of ICT Agreement.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- The trustees will ensure that use of appropriate filters and monitoring systems does not lead to "over blocking", such that there are unreasonable restrictions as to what young people can be taught with regards to online teaching and safeguarding
- Any requests by staff for websites to be added or removed from the filtering list must be authorised by the Business manager.
- All City of Rochester School systems will be protected by up to date anti-virus software.
- Personal use will only be monitored by the DSL, Head Teacher or trustees for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for City of Rochester School purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the staff disciplinary policy.

5. Published Content on City of Rochester School Website:

- The Head Teacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.

6 Network Security:

- Network profiles within Office 365 for each staff member are created, in which the individual must enter a username and personal password when accessing the Office 365 , email and shared space systems within City of Rochester School
- Passwords have a minimum and maximum length, to prevent "easy" passwords or mistakes when creating passwords.

7 Cyber Bullying: 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.)

7.1 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. Form teachers will discuss cyber-bullying with their 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.2 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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, trustees 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.

9 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 Positive 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 disciplinary policy. 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 new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSL's 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.

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.

12. Monitoring arrangements

Staff and the DSL log behaviour and safeguarding issues related to online safety on CPOMs.