Online Safety Policy

Oliver Goldsmith Primary

"Inspiring a love of learning"

Date Reviewed and Ratified: September 2023

Date to be reviewed: September 2024

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 6
5. Educating parents/carers about online safety 7
6. Cyber/Online-bullying 7
7. Acceptable use of the internet in school 8
8. Pupils using mobile devices in school 8
9. Staff using work devices outside school 9
10. How the school will respond to issues of misuse 9
11. Training 9
12. Monitoring arrangements 10
13. Links with other policies 10
Appendix 1: EYFS and KS1 Pupils- Class Computing contract- Acceptable Use Agreement 11
Appendix 2: KS2 Pupils- Class Computing contract- Acceptable Use Agreement 12
Appendix 3: Acceptable use agreement (staff, supply staff, governors and volunteers) 14

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, supply staff, visitors and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 child-on-child abuse or 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 2023, 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.

3. Roles and responsibilities

3.1 The Governing Board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with ICT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually (July each year)
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governors who oversee Online safety and Safeguarding are, Himesh Patel (Our Chair of Governors), Hemal Davda and Fouzia Khan.

All governors will:

- Ensure they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school 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) and 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

- Working with the IT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, IT 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's child protection policy
- Ensuring that any online safety incidents are logged (on CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged (on CPOMS) 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 governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The IT Team- RA Tech

The IT Team are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff, supply staff, and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- 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
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Speaking to the DSL if they have concerns that our school's filtering and monitoring systems are preventing access to any materials they require for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy and our Safeguarding 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.

3.6 Parents/carers

Parents/carers will:

- Have access to this policy via our website
- Be notified of the online safety education the school provides and the pupil acceptable use policy (class computing contract) which pupils are asked to sign and abide by

Parents/carers 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, where relevant, and expected to follow it.

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

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

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/carers about online safety

The school will raise parents/carers' awareness of online safety via our school website, letters or other communications home, where necessary, and as part of Online Safety Parent Time meetings.

6. Cyber/Online-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.

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.

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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in our Safeguarding and Child Protection Policy and our School Behaviour Policy.

6.3 Examining electronic devices

The Headteacher 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 Headteacher 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
- Attempt to make contact with the parents/carers of the pupils involved
- 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 co-operation

If inappropriate material is found on the device, it is up to the Headteacher to decide on a suitable response.

If the Headteacher **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 and together make a decision as to the most appropriate next steps in line with the DfE's latest guidance on searching, screening 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 complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Our school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to upset and bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to upset or bully pupils in line with our Safeguarding and Behaviour Policy.

7. Acceptable use of the internet in school

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 and restrict access through filtering systems where appropriate.

8. Pupils using mobile devices in school

Pupils in Years 5 and 6 may bring mobile devices into school, but are not permitted to use them during:

- lessons
- Clubs
- before or after school, or during any other activities organised by the school

Pupils must turn off their mobile phones when they enter the school site and hand in their mobile phones to their class teacher when they enter the classroom, where they will be stored safely. Pupils' mobile phones will then be handed back to them at the end of the school day and must not be turned on until they leave the school site.

Any use of mobile devices within our school grounds by pupils must be in line with the pupil acceptable use agreement. Use of mobile phones by pupils in Years 5 & 6 is for the purpose of communication between pupils and their parents/carers for safety reasons and not for the purpose of sharing images/videoes etc with their peers.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software when prompted by their computer system or the IT department to do so
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that 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 our IT department and the Headteacher.

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 Behaviour and Safeguarding policy and notify the DSL by reporting the incident on CPOMs. 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 by the Headteacher in accordance with the staff code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All staff members and volunteers will receive training on online safeguarding issues including cyber-bullying and the risks of online radicalisation as part of their annual Safeguarding training/induction..

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 our weekly Goldsmith Gazette, staff meetings, emails and CPD sessions).

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, misogynistic and misandrist messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

The DSL and deputies 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 online safeguarding issues as part of their safeguarding training.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL and Deputy DSLs monitor safeguarding issues related to online safety on CPOMs and through monitoring of the curriculum and behaviour.

This policy will be reviewed every year by Annette McAndrew (the DSL). At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour and Exclusions Policy
- Staff Code of Conduct Policy
- Computing Policy
- RHE Policy
- Data protection policy and privacy notices
- Complaints procedures
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 Pupils- Class Computing contract- Acceptable Use Agreement

Computing Class Contract 2023/2024

Acceptable Use Policy for Class _____

To stay safe online and on our devices:

1. We will look after and use all the school IT equipment properly.

2. We will only use devices or apps, sites or games if a trusted adult says so.

3. We tell a trusted adult if we are scared, worried, or confused about anything we see online.

4. We will use a safe online name and not share our personal information for example name, age or address.

5. We will not talk to people online that we do not know.

6. We will not post or send anything online which upsets other people.

7. We understand that the school can check our use of IT and talk to our parent/carer if they are worried about our online safety.

We confirm that we have read, discussed and will follow this contract:

Names:

Appendix 2: KS2 Pupils- Class Computing contract- Acceptable Use Agreement

Computing Class Contract 2023/2024

Acceptable Use Policy for Class _____

To stay safe online and on my devices:

1. We will always use the school's ICT systems and the internet responsibly and for educational purposes only.
2. We will keep our usernames and passwords safe and not share these with others.
3. We will use a safe online name and not share our personal information for example name, age, address or telephone number.
4. We will tell a teacher (or sensible adult) immediately if we find any material which might upset or harm us or others.
5. We will not talk to people online that we do not know or arrange to meet anyone offline without first consulting our parent/carer.
6. We will not access any inappropriate websites including: social networking sites, chat rooms and gaming sites.
7. We will not create, link to or post any material that is offensive or inappropriate.
8. We understand that the school can check our use of IT and talk to our parent/carer if they are worried about our online safety.

Years 5/6: If we bring a personal mobile phone or other personal electronic device into school:

9. We will turn our mobile phone off when on the school site and hand our phone to our class teacher at the beginning of the day and have it returned at the end of the school day.

10. *We will not use our phone during lessons, clubs or other activities organised by the school*

11. *We will use all devices responsibly- inside and outside of school and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.*

We confirm that we have read, discussed and will follow this contract:

Names:

Appendix 3: Acceptable use agreement (staff, supply staff, governors and volunteers)

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material or create, share, link to or send such material
- 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, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data which I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I understand that the school can monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored.
- I will inform the designated safeguarding lead (DSL – Mrs McAndrew) 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	**Date:**