Online Safety Policy

The staff responsible for the Online Safety Policy is the

Maths & Computing Curriculum Leader Team

The governor responsible for the Online Safety Policy is the

Governor linked to the
Maths & Computing Curriculum Leader Team

Agreed by School Council:

Agreed by staff: December 2020

Agreed by governors: 11th December 2020

Review Date: Autumn 2021

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Ofsted inspectors will always make a written judgement under leadership and management about whether or not the arrangements for safeguarding children and learners are effective.

Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.

1. Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Roydon Primary School with respect to the use of technologies;
- Safeguard and protect the children and staff;
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice;
- Set clear expectations of behaviour and codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community;
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation, etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of the Roydon Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school's technologies, both in and out of Roydon Primary School.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- The policy will be posted on the school website;
- The policy will be included in the school induction pack for new staff, including information and guidance where appropriate;
- All staff must read and sign the 'Staff ICT Code of Conduct' before using any school technology resource. Pupil ICT Code of Conduct (created by Digital Leaders) will be issued to, and signed by, all pupils;
- Regular updates and training on online safety for all staff will be delivered, including any revisions to the policy;
- The Staff ICT Code of Conduct discussed with staff at the start of each academic year.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE).
- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the teaching staff and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

Our school:

- has a clear, progressive online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to the children's age and experience;
- will remind students about their responsibilities through the pupil ICT Code of Conduct;
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism, how to check copyright and that they must respect and acknowledge copyright/intellectual property rights.

Staff training
This school makes regular up-to-date training available to staff on online safety issues and the school's online safety education program via National Online Safety.

3. Incident management

In this school:

- there is strict monitoring and application of the online safety policy, including the Acceptable Use and the Staff Code of Conduct and a differentiated and appropriate range of sanctions;
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security and filtering
In this school:

- we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision;
- we use a Watchguard client firewall that blocks attacks and filters websites in categories. We have different levels of permission depending on the user's needs. By default we have a strict lock-down policy to prevent students accessing inappropriate sites;
- we can tailor our client firewall specifically to block a certain site or a whole category and it is monitored by a third party filtering specialist Alex DeVries. He has access to the router and filter system and would be able to supply reports on request;
- our network and individual technologies are managed by JC Technologies.

Email
Our school:

- provides staff with an email account for their professional use, e.g. @coudworking.org.uk and makes clear personal email should be through a separate account;
- will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law;
- will ensure that email accounts are maintained and up-to-date.

Pupils' email:

- We use school-provisioned pupil email accounts that can be audited.

- Pupils' email addresses are anonymous.
- Pupils are taught about the online safety and etiquette of using email both in school and at home.

School website

- The school web site complies with statutory DfE requirements.
- Most material is the school's own work; where other's work is published or linked, we credit the sources used and state clearly the author's identity or status.
- Photographs of pupils published on the web do not have full names attached. When saving images we do not use pupils' names in the file names or in the tags when publishing to the school website.
- Our website is managed by Creative Corner.

Social networking

Staff, volunteers and contractors:

- Staff are instructed always to keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's Office 365 for such communications.
- The use of any school approved social networking will adhere to Acceptable Use Policy and the Staff Code of Conduct.
- Staff can contact pupils and parents via our approved school membership of Class Dojo. Parents are responsible for the monitoring of their own child's activity on Class Dojo outside of school.

Pupils:

- are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work;
- are required to sign and follow our pupil ICT Code of Conduct.

Parents:

- The school has certified school accreditation from National Online Safety due to the support offered to parents via online learning modules and print out advice.

Digital images and video

In this school:

- we gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school and annually;
- we do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school-produced video materials/DVDs;
- staff sign the school's Staff Code of Conduct and this includes a clause on the use of personal mobile phones/personal equipment;
- if specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.

5. <u>Input from School Council</u>

- The School Council has discussed the importance of avoiding dangers online and how everyone in school can keep themselves safe online.

We learn about online safety during assembly, lessons, safety weeks and the Year 6 children go to Crucial Crew sessions. If you have a problem online you could tell your parent or teacher. Also, you can report any issues on the school website by clicking on the CEOP button.

- *"Make sure you tell a grown up if something goes wrong on your computer that you don't like."* F, Year 2
- *"If you get a text or phone call from someone you don't know, you go to an adult so they can check it or delete it."* E, Year 4
- *"Never share your personal details on the internet."* J, Year 6
- *"If you're using a social media app or site, if you see something inappropriate, you can report it to the CEOP site."* C, Yr. 6