



# Rosh Pinah Primary School

## Online Safety Policy

Ratification by Governing Body: March 2020

## Contents

1. Aims .....	3
2. Legislation and Guidance.....	3
3. Roles and Responsibilities .....	3
4. Educating Pupils about Online Safety.....	4
5. Educating Parents about Online Safety .....	5
6. Cyber-Bullying.....	5
7. Acceptable use of the Internet in School .....	6
8. Pupils using Mobile Devices in School.....	7
9. Staff using Work Devices outside School .....	7
10. How the School will respond to issues of Misuse .....	7
11. Training.....	7
12. Links with other Policies .....	8

## **1. Aims**

Our School aims to:

- Have robust processes in place to ensure the online safety of pupils, Staff, Volunteers and Governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole School Community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

## **2. Legislation and Guidance**

This Policy is based on the Department for Education's (DfE) 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
- Searching, screening and confiscation.

It also refers to the Department'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 Body**

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

All Governors 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.

### **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 DSL 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
- 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 Management 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 Body.

### **3.4 The ICT Manager**

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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.

### **3.5 All Staff and Volunteers**

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

- Maintaining an understanding of this Policy
- Implementing this Policy consistently
- Agreeing and adhering to the terms 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 Management Policy.

### **3.6 Parents**

Parents are expected to:

- 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 factsheet - [Childnet International](#)

### **3.7 Visitors and Members of the Community**

Visitors and members of the community who use the School's ICT systems or internet will be made aware of this Policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

## **4. Educating Pupils about Online Safety**

Pupils will be taught about online safety as part of the Curriculum.

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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant. The School will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

## **5. Educating Parents about Online Safety**

The School will raise parents' awareness of internet safety in letters or other communications home, and in information. This Policy will also be shared with parents.

Online safety will also be covered during parental workshops.

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.

## **6. Cyber-bullying**

### **6.1 Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour Management Policy.)

### **6.2 Preventing and Addressing Cyber-Bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies and workshops.

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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the School will follow the processes set out in the School's Behaviour Management 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.

### **6.3 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

## **7. Acceptable use of the Internet in School**

All Pupils, Parents, Staff, Volunteers and Governors 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.

The School will monitor the websites visited by Pupils, Staff, Volunteers, Governors and Visitors (where relevant) to ensure they comply with the above.

### **8. Pupils using Mobile Devices in School**

Year 6 pupils may bring mobile devices into School, but in line with the Mobile Phone Policy are not permitted to use them on the School premises.

### **9. Staff using Work Devices outside School**

Staff members using a work device outside School must not install any unauthorised software on the device and must not use the device in any way which would violate the School's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside School. Any USB devices containing data relating to the School must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

### **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 Child Protection and Safeguarding Policy and Behaviour Management Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident and will be proportionate.

Where a staff member misuses the School's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

### **11. 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).

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.

More information about Safeguarding Training is set out in our Child Protection and Safeguarding Policy.

## **12. Links with other Policies**

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Management Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Acceptable Use Agreement