Online Safety Policy

February 2023

Contents

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 statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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 and Education for a Connected World: 2020 edition - This curriculum framework provides guidance on supporting children and young people to navigate the digital world safely.

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 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 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 (appendix 2)

3.2 The headteacher

The Executive 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 deputy are set out in our child protection and safeguarding policy.

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

- Supporting the Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Executive headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged on CPOMS (the school's safeguarding and child protection software) and with SLT (Senior Leadership Team), 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 relationship 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

This list is not intended to be exhaustive.

3.4 Computing Leaders and Managers

The Rowan Learning Trust IT manager and Computing Leader 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.
- Conducting a full security check and monitoring the school's ICT systems monthly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- The Computing Leader (with support from Senior Leadership Team) is responsible for:
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.

- Computing Leaders obtain the Annual Certificate in Teaching Online Safety from the National Online Safety Portal
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Relationship policy.

This list is not intended to be exhaustive.

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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure 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 dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher/ Head of School 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 (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- 'What are the issues?' UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- 'Hot topics' Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- 'Parent factsheet' Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
-

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 (appendix 2). Visitors will only be offered the Guest WIFI login if it is required for their work.

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.

In **Key Stage 2,** pupils 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.

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use regular assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. We will also respond to the current interests and needs of our school community.

5. 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. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings and we will also use the resources produced by National Online Safety. Parents will be invited to register for this free resource.

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 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. Teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

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 (see section 11 for more detail).

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.

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 (appendices 1 and 2). 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 Rowan Learning Trust may monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may not bring mobile devices into school unless their parents have insisted, due to walking home alone, for example.. In this situation, the phones must be turned off and handed in at the office, returned at the end of the day. Any breach of this by a pupil may trigger disciplinary action in line with the school relationship policy, which may result in the confiscation of their device. This includes Smart watches that are capable of recording images or sounds.

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, as set out in appendix 2.

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 SMT.

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 the Relationship 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. 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. This will be accessed via the National College:

- Certificate in the Prevent Duty (2022-23) - The National College

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 and deputy 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.

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

12. Data Protection

We have a separate Data Protection Policy that is compliant with the Data protection in schools' publication. Published by the Department for Education 3 February 2023.

https://www.gov.uk/guidance/data-protection-in-schools/responsibilities

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed biannually by the Executive Headteacher. 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
- Relationship policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

Whitley Village School Acceptable Use Policy

We only use the internet when an adult is with us.
We ask permission before using the internet.
We only use websites that our teacher has chosen.
We tell an adult if we see anything we are uncomfortable with.
We immediately close any webpage we are uncomfortable with.
We never give out personal information or passwords.
We never arrange to meet anyone we don't know.

I understand that each time I go on a school device, I agree to all the things mentioned above.

Appendix 2

Acceptable Use of Technology

Code of Conduct

Introduction

ICT in its many forms – internet, email, mobile devices etc – are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly. All staff at Whitley Village Primary School are aware of the following responsibilities:

- All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.

All staff, Governors and visitors understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by its owner. Please refer to the acceptable use policies for further information.

- No staff, Governors or visitors will disclose any passwords provided to them by the school.

- All staff, Governors and visitors understand that they are responsible for all activity carried out under their username.

- Staff, Governors and visitors will not install any hardware or software on any school owned device without the Head's permission.

- All staff, Governors and visitors will only use the school's email / internet / intranet etc and any related technologies for uses permitted by the Head or Governing Body. If anyone is unsure about an intended use, they should speak to the Head beforehand.

- All staff, Governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Head or Governing Body. No passwords should be divulged and only encrypted memory sticks should be used.

- Personal devices must only be used in the context of school business with the explicit permission of the Head. Personal mobile phones or digital cameras must not be used for taking any photographs related to school business. Each class has access to a tablet or digital camera specifically for this purpose. These devices must never be used for personal use.

- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- All staff, Governors and visitors will only use the approved email system for school business, unless otherwise agreed with the Headteacher.

- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. Our parents/carers are asked to sign if they agree to their children's images being used for school advertising, publishing on the website/Twitter feed or in the local press. If a parent/carer does not agree to this, we ensure that their child's photograph is not used.

- All staff, Governors and visitors will make every effort to comply with copyright and intellectual property rights.

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head or the Deputy safeguarding leader in line with our school's Safeguarding Policy.

I acknowledge that I have received a copy of the Acceptable Use of Technology Code of Conduct.

Full Name _____

Signature _____

Date _____