The Acorns
Primary and Nursery School

Mutual respect Equity Inclusivity Love

Online Safety Policy

November 2024

Policy Document Version Control

Responsibility for Policy:	*Deputy Headteacher*
Policy approval/date:	*11/24*
Frequency of Review:	*Annual*
Next Review date:	*11/24*
Related Policies:	*Preventing & Tackling Bullying Policy and our SEND/Inclusion Policy.* *Relationship Policy.*
Minor Revisions:	*Page 8 – added line.*
Major changes	*Page 6 – rewritten sections on pupil and parent education.*
Full re-write	

Mission: Be The Best You Can Be

Vision: Providing A World-Class Start To Life

At The Acorns Primary & Nursery School, we are a Rights Respecting School where everyone is welcome - we have No Outsiders. We equip our pupils with the skills and knowledge they need to become positive, global citizens. During their time here, children develop into intrinsically motivated, life-long learners: they understand the value of working hard and they aspire to achieve.

Our pupils leave us with a strong, moral compass, comfortable in their own skin, and knowing their own minds. They are brimming with self-belief and self-worth and are capable of being in respectful, trusting relationships with others in their community.

Throughout their time at The Acorns, we instil the characteristics of effective learning. These allow our pupils to develop into confident, resilient, and independent adults, prepared to succeed in the modern world.

We achieve this vision through our daily mission - Be The Best You Can Be - and by remaining true to our core values of Mutual respect, Equity, Inclusivity and Love.

Values:

Mutual respect

Equity

Inclusivity

Love

We are a Rights Respecting School with No Outsiders

Article 17: Every child has the right to reliable information from a variety of sources. Every child should be protected from materials that can harm them.

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

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.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the schools' leadership team 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)

Senior Management Team

SMT are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

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 Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with SMT, IT support 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 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

This list is not intended to be exhaustive.

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 IT 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 IT systems monthly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The Computing Leader (with support from SMT) is responsible for:

- 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 dealt with appropriately in line with the school relationship policy

This list is not intended to be exhaustive.

Class Teachers

- Delivering agreed curriculum content designed to inform and develop pupils' understanding of how to stay safe online.

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.

Parents

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
- Information, Advice and Support to Keep Children Safe Online (internetmatters.org)

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.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. We will follow a trusted scheme of work to provide quality learning opportunities for all pupils. Online safety will not only be taught through our Computing curriculum but will also be discretely taught as part of our online safety curriculum.

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. We will also respond to the current interests and needs of our school community.

All staff will receive relevant training to ensure they are confident and comfortable delivering the content within our curriculum.

Educating parents about online safety

Parents will receive relevant feedback and information of what we teach our pupils, what they understand and any wider issues or information we feel they should know. This will be communicated through our School Spider communication systems.

Online safety will also be covered during parents' evenings, where we feel it is appropriate and necessary. This will involve regular support workshops and physical resources (handbooks) that target support for parents setting up new devices and keeping children safe online. These will be sources from trusted organisations.

If parents have any queries or concerns in relation to online safety, they are encouraged to communicate this with school staff.

When necessary, school will involve outside agencies (social care / police) to support in matters that should not be dealt with by school.

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 relationship policy.)

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.

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.

Pupils using mobile devices in school

Pupils may bring mobile devices into school but are not permitted to use them at any point during the school day. They must be taken to SMT at the start of the school day and collected at home time. 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. Parents will always be informed of any actions taken by school staff, and the reasons for these actions.

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 SMT.

Work devices must be used solely for work activities.

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.

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.

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

Monitoring arrangements

All staff can log behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed Annually by the Deputy Headteacher. At every review, the policy will be shared with the governing board.