THE ROBERT DRAKE PRIMARY SCHOOL

E-SAFETY POLICY

This policy is based on the Department for Education (DFE's) statutory safeguarding guidance: Keeping Children Safe in Education Document Annex C, and its advice for schools about: Teaching Online Safety in Schools, Preventing and Tackling Bullying, Cyber-Bullying. Advice for Headteachers and School Staff, Searching, Screening and Confiscation and advice published by the UK Council for Online Safety. It should also be read in conjunction with the school's Behaviour Policy, Safeguarding Policy, Appropriate Use Policy and Social Media Policy.

Aims

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Filters and Monitoring

The Robert Drake Primary school uses filtering and monitoring systems that are supplied with the broadband service provided by RM Safety Net. This system regularly monitors the traffic on the network and the use of certain websites and search topics are restricted. The school also uses 'child friendly' search engines such as swiggle.co.uk which is recommend by South West Grid for Learning (SWGL).

Full details of the school's filtering and monitoring procedures can be found in the Filtering and Monitoring Policy.

Information and Support for Parent, Staff and Governors

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, letters, newsletters, website updates, guest speakers and information about e-safety campaigns.

Roles and Responsibilities

The Governing Body

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

The Governing Body 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).

The Governing Body 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 IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

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

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 3);
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college 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;

- Ensure that there are robust online safety tools in place (including strategic oversight of filtering and monitoring systems to support this).

The Co-Headteachers

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

- Ensure that there are robust online safety tools in place (including strategic oversight of filtering and monitoring systems to support this);
- Safeguarding procedures are robust and in place for online safety incidents.

The Designated Safeguarding Lead

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;
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks;
  - Working with the headteacher, ICT 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 child protection policy;
  - Ensuring that any online safety incidents are logged (see appendix 5) 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;
- Ensure that there are robust online safety tools in place (including strategic oversight of filtering and monitoring systems to support this);
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

The ICT Manager

The ICT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 monthly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- 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 dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

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 of the school's Appropriate Use Policy;
- 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 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.

Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- Understand that their child has read, understood and agreed to the terms of the school's Appropriate Use Policy.

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

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 of the Appropriate Use Policy.

Teaching of Online Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the Computing Curriculum;
- Key e-safety messages are reinforced as part of a planned programme of assemblies and activities;
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Pupils will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Through the promotion of British Values and the Prevent Duty the pupils will be taught to challenge extremist views when using material accessed on the internet;
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

From the National 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.

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.

Cyber-bullying

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 1 person or group by another person or group, where the

relationship involves an imbalance of power. (See also the school's Behaviour 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.

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.

The school also sends information 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining Electronic Devices – Searching Screening and Confiscation

The school will follow guidance from Searching, Screening and Confiscation DfE 2022, UKCIS guidance and school's Behaviour Policy 2022.

The headteacher, and any member of staff authorised to do so by 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 authorised staff member 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. If the search is not urgent, they will seek advice from one of the Co-Head Teachers
- 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

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **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 (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching 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 searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's behaviour policy / searches and confiscation policy

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

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;
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- 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;
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way which 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 the ICT Manager.

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.

The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Robert Drake Primary will treat any use of AI to bully pupils in line with our Anti-Bullying and Behaviour Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Data Protection

In line with the school's Data Protection Policy, all staff and governors must be aware of the risks posed by data being accessed by unauthorised people. All members of staff and governors must take appropriate steps to minimise this risk by ensuring that all data is kept on password encrypted memory sticks and disposed hard drives are securely destroyed by registered companies when no longer required.

Further information can be found on the following websites:
www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk
http://educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation
www.gov.uk/UKCCIS

Date Reviewed: Autumn 2024
Date of Next Review: Autumn 2025