



ONLINE SAFETY POLICY

Review Date September 2026			
Statutory Policy? No	Governors Approval Yes	Responsibility of Lara Collingwood	Date September 2025

1. Aims

1.1 Fort Royal Primary School aims to:

- Have robust processes in place to ensure the online safety of children, staff, students, visitors 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, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

1.2 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** - being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** - being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [Internet-Matters-Report-Vulnerable-Children-in-a-Digital-World.pdf \(internetmatters.org\)](#)

It also refers to the DfE'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 considers 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.

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). This will be planned during the Safeguarding Governors termly meetings with the DSL.

The governor who oversees Safeguarding and Online Safety is Robyn Chris Percival.

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms of Fort Royal Primary School's IT Acceptable Use Policy.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that all children at Fort Royal Primary School are taught about safeguarding, including online safety, in an appropriate way in line with their level of development. 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, especially for our children at Fort Royal Primary School.
- Ensure that the school has robust monitoring and filtering arrangements in place.

3.2 The Headteacher - Ed Francis

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 - Lara Collingwood

Details of the school's designated safeguarding lead (DSL) deputies 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, IT 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 1) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of online-bullying are logged and dealt with appropriately in line with the [Anti-Bullying policy](#).
- Deliver staff training on online safety annually and update them on any online safety issues regularly through emails or staff briefings.
- 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.
- Ensuring that parents are kept up to date with online safety issues and offer advice to parents through the schools early help offer.
- Monitoring and reviewing the schools monitoring and filtering systems on a regular basis.

This list is not intended to be exhaustive.

3.4 The IT manager - Andy Toy

The IT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering (Watchguard) and monitoring (SENSO) systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure children 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 regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Working closely with the DSL to ensure that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy.
- Monitoring and reviewing the schools monitoring and filtering systems on a regular basis with the DSL.

This list is not intended to be exhaustive.

3.5 All staff, students and visiting professionals

All staff, including students, contractors and agency staff, and visitors are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agree and adhere to the terms of Fort Royal Primary School's IT Acceptable Use Policy.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 1) 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 [Anti-Bullying policy](#) and logged in a timely manner on CPOMS.
- 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' and following the school [Child on Child Abuse policy](#).

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Contact school if they have any concerns about their child's online activity and ask for advice and support.

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 resource sheet - [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 and adhere to the terms of Fort Royal Primary School's IT Acceptable Use Policy.

4. Educating children about online safety

Children will be taught about online safety as part of the curriculum and it is embedded into all areas of the curriculum when ICT is being used, but also taught discreetly through online safety activities, when appropriate - follow link:

[e-safety-progression.pdf \(primarysite-prod-sorted.s3.amazonaws.com\)](https://primarysite-prod-sorted.s3.amazonaws.com/e-safety-progression.pdf)

We also teach elements of online safety as part of our PSHECC curriculum in the Autumn 2 term each year - see overview:

[pshecc-with-smisc-british-values-links.pdf \(primarysite-prod-sorted.s3.amazonaws.com\)](https://primarysite-prod-sorted.s3.amazonaws.com/pshecc-with-smisc-british-values-links.pdf)

Children working within Layers of Learning 4-8, 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.

Children working within Layers of Learning 9-16, will be taught to:

- ✓ Use technology safely and respectfully, keeping personal information private.
- ✓ Know where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

The safe use of social media and the internet will also be covered in other subjects where relevant or if an individual concern is raised to the DSL. Where necessary, teaching about safeguarding, including online safety, will be adapted for our children and victims of abuse.

As a whole school we will celebrate Safer Internet Day and there will also be assemblies around online safety.

Each classroom will display online safety posters for adults to refer to when children are accessing the internet (see Appendix 3).

5. Educating parents about online safety

The school will raise parents' awareness of internet safety through the school fortnightly newsletter, The Fort Royal Flyer or other communications home, and in information via our website or social media. This policy will also be shared with parents.

Online safety will be covered through a workshop once a year by the Family Support Worker and information will be available at Parents' Evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with a member of the safeguarding team.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Online-bullying

6.1 Definition

Online-bullying is the use of technology (social networking, messaging, text messages, e-mail, chat rooms etc.) to harass threaten or intimidate someone for the same reasons as stated above.

Online bullying can take many forms including:

- Abusive or threatening texts, emails or messages
- Posting abusive comments on social media sites

- Sharing humiliating videos or photos of someone else
- Spreading rumours online
- Trolling - sending someone menacing or upsetting messages through social networks, chatrooms or games
- Prank calls or messages
- Group bullying or exclusion online
- Anonymous messaging

6.2 Preventing and addressing online-bullying

To help prevent online-bullying, we will ensure that, where appropriate, children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children 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 online-bullying with children (where appropriate), 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 online-bullying. We will do this through our PSHECC curriculum.

All staff, governors and students (where appropriate) receive training on online-bullying, its impact and ways to support children, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of online-bullying, the school will follow the processes set out in the school [Anti-Bullying policy](#). All online bullying concerns will be logged on CPOMS. Where illegal, inappropriate or harmful material has been spread among children, 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.

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 children's 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 children will be carried out in line with the DfE's latest guidance on screening, searching and confiscation [Searching, Screening and Confiscation \(publishing.service.gov.uk\)](#).

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

7. Acceptable use of the internet in school

All staff, visiting professionals, students and governors are expected to agree and adhere to the terms of Fort Royal Primary School's IT Acceptable Use Policy.

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.

We will monitor the websites visited by children, staff, students, governors and visitors (where relevant) to ensure they comply with the above.

8. Children using mobile devices in school

Fort Royal Primary School does not advocate children bringing personal mobile devices into school. Where this does happen, the pupil will be encouraged to understand that the mobile phone must be handed in to the class teacher, where it will be stored in the main school office or a locked cupboard, and that it will be returned to their passenger assistant / parent / carer at the end of the school day. A member of staff will call the pupil's parents to explain that we would prefer personal mobile devices are not sent into school with their child.

9. 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, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- 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.
- 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 Andy Toy the IT manager or a member of staff from ICT4.

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 policies on internet acceptable use. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

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 low level concerns policy, staff disciplinary procedures and/or the 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 online-bullying and the risks of online radicalisation.

All staff members will receive annual refresher online safety training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages.
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
 - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure children can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, once a year. They will also update their knowledge and skills about 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.

Students will receive appropriate training and updates, if applicable.

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

12. Artificial Intelligence (AI)

We are living through a period of significant technological change, with artificial intelligence (AI) beginning to reshape how we lead, communicate and deliver education. From streamlining administrative processes to supporting operations, workload, teaching, CPD, inclusion and personalised learning, AI offers real potential to enhance the way school function and support staff in powerful new ways. At Fort Royal Primary School we will ensure that we plan for the safe and effective use of AI so it benefits all of our staff. We consider the following points:

- ✓ Safety - assessing suitable tools, safeguarding, data protection, intellectual property
- ✓ Opportunities - reducing workload,
- ✓ Embedding AI into your digital strategy - CPD, digital standards
- ✓ DfE guidance - policy paper, product safety framework, data protection guidance, KCSIE, digital standard

We will take account of the following DfE guidance:

[Using AI in education settings: support materials - GOV.UK](#)

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 1.

This policy will be reviewed every year by the Designated Safeguarding Lead in line with current guidance from [Keeping Children Safe in Education](#).

14. Links with other policies

This Online Safety policy is linked to our:

- Child protection and safeguarding policy
- Relationship based Behaviour and Regulation policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Low Level Concern Policy
- Mobile Phone Policy
- IT Acceptable Use Policy
- Confidential Reporting (Whistle Blowing) Policy
- Anti-Bullying
- Child on Child Abuse Policy

Appendix 1:

Fort Royal

Community Primary School

Play, Learn, Laugh, Succeed

ONLINE SAFETY INCIDENT LOG

[illegible]

Appendix 2:



Mobile Phone Policy

When mobile phones are misused, it can impact on an individual's dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of all.

All Staff:

- Are not permitted to use their own mobile phones to contact children or those connected with the family of a pupil. Staff should use a school phone where contact with parents or carers is necessary
- Staff are not permitted to make or receive calls or texts during contact time with children. Emergency contact should be made via the school office. Should there be exceptional circumstances then staff should make the Head teacher or a member of SLT aware of this and may be able to have their phone in case of having to receive an emergency call.
- Will use mobile phones in designated areas such as the staff room or in a private room away from children, regardless of the time of day
- Should ensure that their phones are protected with an access codes in case of loss or theft
- Are not at any time permitted to use recording equipment on their mobile phones. Legitimate recordings and photographs should be captured using school equipment such as cameras and iPads.
- Should report any usage of mobile devices that causes them concern to the Head teacher.
- When wearing an Apple Watch or any other smart watch all staff are to ensure that it is on silent and that the message and phone app's have been disabled during the school day.

If any staff member breaches the school policy then disciplinary action may be taken, if appropriate.

Responsibility: Headteacher.

Appendix 3

 STAY  SMART  ON LINE!												
 Safe	 Keep	 all of	 your	 personal information	 safe.							
 Meet	 Don't meet	 with	 strangers	 you	 have talked to	 online.						
 Accept	 Think	 before	 you	 accept	 anything	 online.						
 Reliable	 Not	 everyone	 is reliable.	 They	 may	 not	 be	 who	 they	 seem	 to	 be.
 Tell	 Tell	 a	 responsible	 adult	 if	 you	 feel worried	 or	 you're	 not sure.		