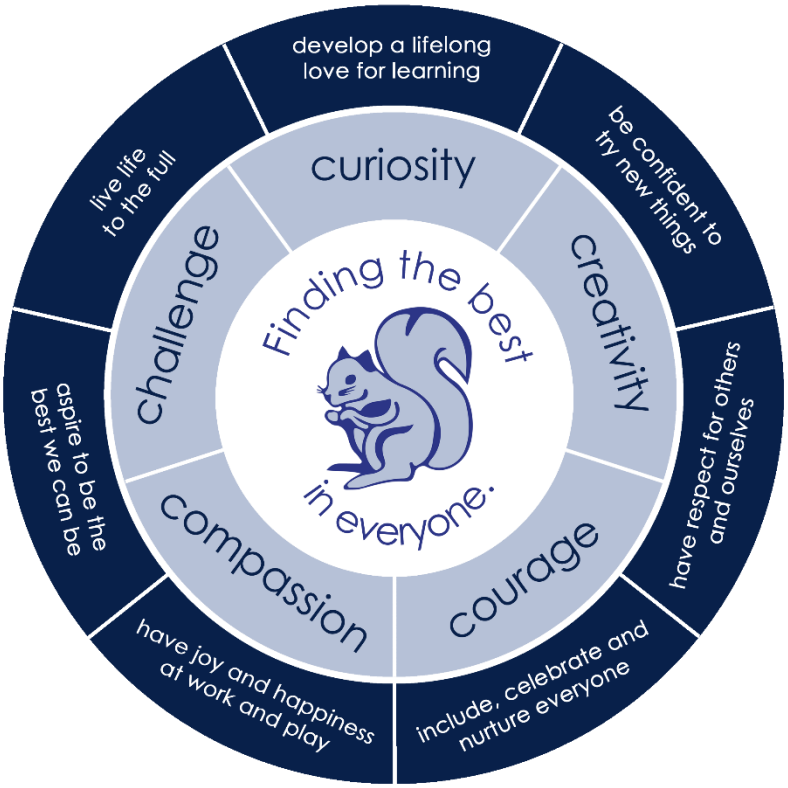
Felbridge Primary School

Finding the best in everyone.

Online Safety Policy
Autumn 2025



This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Revised/Written by:	Emma Thorp
Discussed and approved by Teaching & Learning Committee *(New policy/major revision: committee approval. Annual check: single governor)*	Autumn 2025
Policy check (annual)	Autumn 2026
Date for Full Review (3 years)	January 2028
Status	Non statutory but linked to safeguarding policy

Felbridge Primary School
Online Safety Policy

1. Policy Aims

This policy has been written by Felbridge Primary School, building on a Key model template and models for acceptable use policies / safe internet use guidelines based on County Council documents.

The purpose of our online safety policy is to:

- Safeguard and protect all members of the school community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Felbridge Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content
    - *such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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*
- **Commerce** – financial risks
    - *such as online gambling, inappropriate advertising, phishing and/or financial scam. Examples in our context will include education about the dangers of in-app purchasing*

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
- Relationships and sex education
- Searching, screening and confiscation
- Filtering and Monitoring standards for schools

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 takes into account the National Curriculum computing programmes of study.

3. Policy Scope

- Felbridge Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Felbridge Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Felbridge Primary School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, senior leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of Felbridge Primary School (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as work laptops or mobile devices/tablets.

4. Links with other policies and practices

This policy links with several other policies, practices and action plans including but not exclusively:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and the Code of conduct
- Behaviour policy
- Safeguarding and Child Protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), and Relationships and Sex Education (RSE)
- GDPR

5. Monitoring and Review

- Technology in this area evolves and changes rapidly. The school will therefore check this policy annually and review/re-write as necessary every three years.
    - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteachers are informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes, through the use of termly safeguarding meetings with the Headteacher/DSL/Online Safety Lead.
- Any issues identified via monitoring will be incorporated into our action planning.

6. Roles and Responsibilities

The governing body

The governing body, through the Teaching & Learning governor, has overall responsibility for monitoring this policy and holding the headteachers to account for its implementation.

All governors will:

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet, including their school-issued email account.

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations.
- ensure that appropriate filtering and monitoring systems are in place, while being mindful that they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. (KCSiE 2025)

Headteacher

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

With the governing body, the headteachers and wider leadership team

- have responsibility for ensuring that staff have an awareness and understanding of the filtering and monitoring provisions in place;
- know how to manage these systems effectively; and
- know how to escalate concerns when identified.

The designated safeguarding lead

Details of the school's DSL and deputies (DDSLs) are set out in our safeguarding and child protection policy.

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

- Ensuring staff understand this policy and that it is being implemented consistently throughout the school
- Working with 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 (through use of CPOMS and by informing TLT IT department) 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 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 through the use of termly safeguarding meetings with the governor responsible for safeguarding.

The DSL will undertake specific Online Safety training provided by an appropriate body, for example, The National College.

The DSL and Deputy DSLs will undertake child protection and safeguarding training, which includes aspects of online safety, as provided by Surrey County Council every 2 years. A member of the DSL team also attends regular update meetings provided by Surrey County Council.

The ICT manager

At Felbridge, ICT and hardware management is contracted to an external support company, Eduthing and overseen by the IT department at Tandridge Learning Trust. The Office Manager (who is also a DDSL) has primary responsibility for liaising with the external support company.

The external support company, liaising with and under the direction of the school, 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 security checks and monitoring the school's ICT systems on a regular basis
- Blocking access *(via use of Smoothwall filtering system)* to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Working with the DSL to investigate, log and deal with online safety or cyber-bullying incidents in line with this policy, other relevant policies and the latest KCSiE guidance as appropriate.

Staff and volunteers

All staff, including contractors and agency staff, and volunteers where applicable, 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 (see appendices)
- Working with the DSL to ensure that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with in line with 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.'
- Having an awareness of filtering and monitoring systems, their purpose, benefits and limitations, and reporting any concerns (including sites which may need to be added to block lists) to the leadership team and/or DSLs as appropriate.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher 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, issued on joining the school and/or in Year R and Year 3.

Parents can seek further guidance on keeping children safe online from a variety of organisations and websites. The school will signpost to such resources using the newsletter or if a particular issue necessitates further guidance. Examples of useful and appropriate resources include:

- 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 usually via agreeing to a visitor acceptable use agreement, and expected to follow it.

7. Education and Engagement Approaches

Education and Engagement with Learners

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study. At Felbridge this is facilitated through the use of the **Kapow** Online Safety programme and through discussions as part of regular computing lessons using the **Kapow** schemes of work or the school's PSHE scheme (1decision). The school may also highlight specific online safety topics through events such as **Safer Internet Day** and **NSPCC assemblies/workshops.**
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in classrooms.
- Informing learners, at their level, that network and internet use will be monitored for safety and security purposes.
- Rewarding positive use of technology through praise and use of school reward systems.
- Implementing appropriate peer education approaches, including through group work in class, and using the support of older students where appropriate.
- Seeking pupil voice when writing and developing policies and practices, for example in the development of anti-bullying resources.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable Learners

Felbridge Primary School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Felbridge Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. Kapow schemes of work, as currently used in school, include extensive notes on adaptation and support which could be included when needed.

Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates as part of existing safeguarding and child protection training.
    - This will cover the potential risks posed to learners (the '4 Cs') as well as our professional practice expectations.
    - An understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
    - Staff will also 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

- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to age and ability of learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

Awareness and engagement with parents and carers

Felbridge Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats, including the provision of face-to-face meetings where there is sufficient take-up.
- Drawing their attention to the online safety policy, expectations and current guidance/hot topics in newsletters, letters, and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

8. 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 behaviour policy and anti-bullying 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.

Opportunities to use aspects of the curriculum to cover cyber-bullying may also include personal, social, health and economic (PSHE) education through the use of the 1decision programme, 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. Teachers will undertake further online training specifically related to online safety.

The school may also provide information on cyber-bullying to parents including signs, how to report it and how they can support children who may be affected. This will usually be via information supplied in newsletters.

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.

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.

In our setting, children do not have personal devices on their person in school (older children may have permission to have a device which is stored in the office during the day).

Therefore, 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 to contravene the school behaviour policy.

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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils, if deemed necessary, will be carried out in line with relevant DfE 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.

9. Acceptable use of the internet in school

All pupils, parents, staff and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see appendices). Visitors and volunteers 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.

We will 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 (see separate documents).

10. Filtering and Monitoring

Keeping Children Safe in Education includes guidance around the duty to provide and monitor appropriate filtering and monitoring systems for the school's IT systems and internet access.

Responsibilities regarding this guidance are contained above in the 'roles and responsibilities' section.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs.

Our filtering provider is Smoothwall. We receive daily updates and follow-up any breaches immediately.

11. 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 devices and accounts 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);
- Not sharing the device among family or friends;
- the use of 'multi-factor authentication' when accessing emails through a browser or the Outlook app.

The school may also take measures to ensure that devices intended for staff use outside school are protected, including but not limited to:

- Using settings so that the device locks if left inactive for a period of time
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date

Staff members must not use the device in any way which would violate the school's terms of acceptable use or the staff code of conduct.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they can seek advice from the External Support Company (Eduthing) who is responsible for ICT management by logging a ticket through the given email. The Office Manager and Headteacher can also offer basic advice before deciding whether to log a support ticket.