



Online Safety Policy

Date Policy Formally Agreed By Governors:
Date Policy Becomes Effective: 2017
Review Date: 2018, 2019, 2020, 2023, 2025
Person Responsible for Implementation and Monitoring: Headteacher

1. Aims

Keeping children safe in education 2022: Statutory guidance for schools and colleges (Department for Education (DfE, 2022) states that it is essential that children are safeguarded from potentially harmful and inappropriate online material. Online Safety encompasses the use of technology on a wide variety of devices. Teaching online safety in school Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (DfE, 2019) advises that 'The online world develops and changes at great speeds. New opportunities, challenges and risks are appearing all the time ... it is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.' Online safety enables us to provide safeguards and awareness for all users to control and enhance their online experiences. It is not just about the risks and how we avoid them; it is about ensuring everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks, whilst continuing to benefit from the opportunities.

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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

This policy aims to ensure that:

- there are agreed expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- all members of the school community are aware of their responsibilities and understand how they should use digital technologies responsibly, protecting themselves and the school
- staff help to safeguard pupils online
- clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms are in place
- pupils are prepared to be safe and responsible users online

2. **Roles and Responsibilities**

Online safety is a safeguarding issue not a computing issue. All members of the school community have a duty to be aware of online safety at all times and to know the required procedures and to act on them. The following responsibilities demonstrate how each member of the community will contribute.

The Governing Board is responsible for:

- ensuring the effectiveness of the policy
- being aware of the current issues in online safety
- reviewing (anonymised) incidents and if possible, filtering and monitoring logs

The governor who has the responsibility for Online Safety will closely monitor this area and regularly meet with the Headteacher to discuss the above which will be fed back to the rest of the governing board when necessary.

The Headteacher is responsible for:

- ensuring that all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring
- having a duty of care for ensuring the online safety of members of the school community and fostering a culture of safeguarding
- ensuring that the online safety curriculum is planned, taught, monitored and assessed effectively

The Designated Safeguarding Lead /Deputy Designated Safeguarding Lead (DSL/DDSL) is responsible for:

- being aware of the potential for serious safeguarding issues to arise from: sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming, online bullying
- taking day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- promoting an awareness of, and commitment to, online safety both in school and out
- advising staff and all other members of the school community on matters of online safety
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- reviewing reports of online safety incidents and acting accordingly to these

Staff are responsible for:

- reading, understanding and implementing this policy
- ensuring all online safety incidents, including sexual violence/harrassment, are logged on CPOMS
- maintaining a professional level of conduct in the personal use of technology and model safe and responsible behaviours in their own usage.

Technical Staff (Primary Tech) are responsible for:

- reading, understanding and contributing to this policy
- providing and taking responsibility for a safe and secure technical infrastructure to support learning and teaching by ensuring that appropriate physical access controls exist to control access to information systems, networks and telecommunications equipment situated within school
- ensuring that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- maintaining an awareness of current online safety issues, legislation and guidance relevant to their work and pass any such information to the Headteacher
- reporting any online safety related issues to the Headteacher
- ensuring that provision exists for misuse detection and malicious attack
- documenting all technical procedures and review them for accuracy at appropriate intervals
- restricting all administrator level accounts appropriately

Parents/Carers are responsible for:

- helping and supporting the school in promoting online safety
- consulting with the school if they have any concerns about their children's use of technology
- taking responsibility for their own awareness in relation to the opportunities and risks posed by new and emerging technologies and model safe and responsible behaviours in their own usage
- discussing online concerns with their children, showing an interest in how they are using technology and encouraging safe and responsible usage
- completing the Google Form to acknowledge that they have read, understood and agree with the Acceptable Use Policy before their child starts at the school and to update their agreement as and when the policy/statements are updated.

Visitors, volunteers and members of the school 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 adhere to it and the Acceptable Use Policy and Statement.

3. Procedure for Logging Online Safety Incidents

Any online safety incidents in relation to the categories of risk set out in this policy must be reported immediately to the Headteacher/DSL or DDSL either face to face, where necessary or logged via CPOMS.

The log must state which category of risk the incident relates to as well as all other necessary information as any other safeguarding incident (e.g. name/s of child/ren involved, date, time and location of incident). The Headteacher/DSL or DDSL will use the log of information to further investigate the incident and this may involve checking the filtering and monitoring logs and/or speaking with children and parents.

4. Teaching and Learning

Keldmarsh Primary School believes that the key to developing safe and responsible behaviours online, not only for children but everyone within our school community, lies in effective education. We understand that the internet and other technologies are embedded in our children's lives both in school and out and it is our duty to prepare them to be safe online. Children will be taught about online safety as part of the curriculum within, but not limited to Computing and Personal Development:

In Key Stage 1, children 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, children 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, children 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
- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- where and how to report concerns and get support with issues online.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Parents/Carers

The school will raise parents' awareness of internet safety in letters home, and in information via the school's website and Instagram account. This policy will also be shared with parents/carers and if they have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/DSL and/or the DDSL. A partnership approach will be encouraged with parents which may include practical sessions as well as suggestions for safe internet use at home.

5. Online child on child abuse

Online child on child abuse is any form of child on child abuse with a digital element, for example, sexting, online abuse, coercion and exploitation, child on child grooming, threatening language delivered via online means, the distribution of sexualised content and harassment. The Behaviour Policy and Statement of Behaviour Principles outlines Keldmarsh Primary School's procedures for managing these areas of online safety.

Cyber-bullying

Cyber-bullying is a form of bullying which takes place online, such as through social media 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. Section five of the Behaviour Policy and Statement of Behaviour Principles outlines Keldmarsh Primary School's procedures for dealing with this specific online safety area.

6. Acceptable Use

All pupils, parents, staff, volunteers and governors must sign an Acceptable Use Statement in relation to use of the school's ICT resources, including the internet. Further information is set out in the Acceptable Use Policy.

7. Filtering Internet Access

Keldmarsh Primary School use a filtered internet service provided by Securly. The provision includes filtering appropriate to the age and maturity of pupils and we are proactive regarding the nature of content which can be viewed. Keldmarsh Primary School has a clearly defined procedure for reporting breaches of filtering: these are to be logged as incidents on CPOMS and reported directly to the Headteacher/DSL or DDSL. If a user discovers a website with inappropriate or potentially illegal content, these are to be immediately reported. Such incidents will be reported to appropriate agencies including the filtering provider, the local authority, Child Exploitation and Online Protection (CEOP) or the Internet Watch Foundation (IWF).

8. Policy Review

This policy is reviewed and updated regularly to meet the changing needs of the school and in light of any new initiatives. The last review took in place in January 2025.