



LEAGRAVE PRIMARY SCHOOL

'STRIVING FOR EXCELLENCE, LEARNING FOR LIFE'

Online Safety Policy

Ratified by Governors

Date: October 2026

Document Status	
Author	D.Bastin
Date of Origin	2016
Revised	October 2026
Version	9
Review requirements	Annually
Date of next Review	October 2027
Approval Body	Governing Body
Publication	School Website/ Staff Pack

NON-STATUTORY

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations

Introduction

This Online Safety Policy should be read in conjunction with the Internet Acceptable Use Policy, Social Media Policy, Anti-Bullying Policy, Safeguarding Children and Child Protection Policy including Child Protection, Behaviour Policy, Mobile Devices Acceptable Use Policy and the School's Code of Conduct.

Leagrave Primary School has appointed an Online Safety Coordinator. Within this role, they will attend training that is relevant to the post. They will then cascade this information to all staff, as appropriate.

Our Online Safety Policy has been written by the school's ICT manager and Online Safety Co-ordinator in accordance with the Luton Safeguarding Children Partnership's (LSCP) Online Safety Policy and Government guidance.

Leagrave Primary School staff will take all reasonable precautions to prevent access to inappropriate material in school. However, due to the international scale and linked nature of online content, it is not possible to guarantee that unsuitable material will never appear on a device connected to the school network. Neither the school nor the LSCP can accept liability for any material accessed, or any consequences of online access.

We will audit computer and other device use to establish whether the Online Safety Policy is adequate and that the implementation of this policy is appropriate and effective. This will be carried out by the Headteacher, ICT manager and Online Safety Coordinator.

Why the online and digital communications are important

The online world is an essential element in 21st century life for education, business and social interaction. Leagrave Primary School welcomes its duty to provide its pupils with quality online access as part of their learning experience. Being online is a daily experience for most children in this school. Internet use is a part of the curriculum and a necessary tool for staff and pupils. Almost all homework is set online, although hard copies of homework may be given to children with SEN or who do not have access to a device at home. When classes cannot be taught in school, Google Classroom is used for teaching and learning. (Cross reference the Homework Policy)

Online use enhances learning

The school's internet access is designed expressly for children's use and includes filtering appropriate to the age of children. Pupils are taught how to be safe online and what online use is acceptable and what is not and are given clear objectives for online use. Throughout the school, we follow the Digital Literacy Scheme. This provides pupils with skills and knowledge to access the internet safely, building on their knowledge and skills from one year to the next.

Aims of this Policy

The aims of this policy are to:

- Ensure that pupils benefit from all learning opportunities offered online and from being online in a safe and controlled manner.

- Ensure that all staff and pupils have clear guidance on safe use of all Information Communication Technology (ICT).

Our ICT vision

We will develop the learning environment to provide a range of ICT opportunities and devices. This will educate and empower our pupils to make relevant and safe choices when being online on any devices that they use at school, at home or elsewhere.

Filtering and Monitoring

The Governing Body has overall strategic responsibility for ensuring that the school has appropriate filtering and monitoring systems in place. A member of the Senior Leadership Team (SLT) and a governor will have responsibility for ensuring that the Department for Education's filtering and monitoring standards are met.

The Designated Safeguarding Lead (DSL) is responsible for online safety as part of their safeguarding responsibilities and will lead on safeguarding matters arising from filtering and monitoring. The DSL will work closely with the ICT Manager and filtering and monitoring provider to ensure that safeguarding and technical expertise are combined effectively. Filtering arrangements will also take account of the school's Prevent Duty risk assessment.

The school will maintain appropriate filtering and monitoring systems to safeguard pupils from illegal, inappropriate and potentially harmful online content and activity, without unreasonably restricting teaching and learning.

The effectiveness of the school's filtering and monitoring provision will be formally reviewed at least once every academic year and sooner where a safeguarding risk is identified, working practices change, significant technical changes are made, or new technology, including generative AI, is introduced. The review will consider the needs and risk profile of pupils, including their age and any additional vulnerabilities, and whether the systems provide appropriate protection across all relevant school-managed devices and services, including those used away from the school site.

As part of the review, the school will consider whether its systems can appropriately filter or monitor real-time, dynamic, personalised and AI-generated content. The limitations of filtering and monitoring systems will be recognised and managed through appropriate supervision, staff awareness, pupil education and additional safeguards where necessary.

Filtering and monitoring checks will be carried out and recorded at a frequency appropriate to the school's safeguarding risks. Records will identify when the check took place, who completed it, what was checked and any resulting action. Monitoring arrangements will include weekly monitoring reports highlighting incidents and the immediate reporting of incidents classed as high risk. Any safeguarding concerns identified through filtering or monitoring will be brought promptly to the DSL, recorded and responded to in accordance with the school's safeguarding and child protection procedures.

The school will work with its filtering and monitoring provider and ICT support to ensure that systems are maintained, regularly checked and remain appropriate, effective and reasonable. Filtering will apply appropriately to school-managed devices and users, and checks will ensure that systems have not been disabled or incorrectly configured.

All staff will receive appropriate filtering and monitoring training as part of their safeguarding and child protection training so that they understand the expectations relevant to their roles and responsibilities. Staff supervising pupils using technology will maintain appropriate awareness of pupils' online activity, including what is displayed on their screens. Staff must report any safeguarding concern, inappropriate content, apparent failure of filtering or monitoring, or unreasonable restriction affecting teaching and learning in accordance with the school's reporting procedures.

Virus protection and other appropriate cyber security measures will be maintained and updated in accordance with the school's wider IT and cyber security arrangements.

Artificial Intelligence (AI) in School

The school recognises that Artificial Intelligence (AI) is a rapidly developing area of technology that can provide valuable opportunities for teaching and learning, while also presenting new risks relating to safeguarding, online safety, data protection and the reliability of information.

In line with *Keeping Children Safe in Education (KCSIE) 2026* and relevant Department for Education and UK Council for Internet Safety (UKCIS) guidance, the school will ensure that the use of AI supports pupil wellbeing, protects personal data and is consistent with our safeguarding responsibilities.

AI tools used in school will be considered as part of the school's filtering and monitoring arrangements. The school recognises that AI services can produce real-time, dynamic and personalised content and that traditional filtering systems may not always identify or block inappropriate AI-generated material. The DSL and ICT Manager will therefore consider the risks presented by AI when reviewing the effectiveness of the school's filtering and monitoring systems.

No AI tools or services will be allowed on any school devices without the permission of the Headteacher. (see AI policy)

Before new AI tools or services are introduced for pupil use, the school will consider their suitability, including age restrictions, privacy and data protection requirements, the content they may generate and whether existing filtering and monitoring arrangements provide appropriate safeguards. Where necessary, additional controls or supervision will be put in place. Staff will remain responsible for appropriate supervision of pupils using AI. They should not assume that content generated by an approved AI service is automatically accurate, appropriate or safe. Any inappropriate, harmful or concerning AI-generated content encountered by a pupil or member of staff must be reported in accordance with the school's safeguarding and filtering and monitoring procedures.

The school will regularly review the use of AI and its associated risks, including when new AI technologies or services are introduced or when there are significant changes to existing systems. These reviews will inform the school's wider filtering and monitoring arrangements and any necessary updates to safeguarding, online safety, behaviour, data protection and acceptable use procedures.

Pupils will be taught to use AI safely, responsibly and critically as part of their online safety and digital literacy education. This will include understanding that AI-generated information

may be inaccurate, misleading or inappropriate; protecting personal information; recognising appropriate and inappropriate uses of AI; and knowing how to report content or interactions that cause concern.

(Cross reference AI policy for further details)

Ensuring pupils online access is safe and appropriate

The internet is a communications medium that is freely available to any person wishing to send e-mail or publish a web site, engage in social media, make and watch video clips etc. and in common with other media such as magazines, books and videos, some of the material available is unsuitable for children. The measures outlined below are designed to ensure that our pupils do not encounter upsetting, offensive or otherwise inappropriate material when they are online.

- Current internet access is provided by Virgin Media through Atomwide. This is a service designed for children including a “firewall” filtering system intended to prevent access to material that is inappropriate for children.
- Pupils working online always work in the presence, and under the guidance, of the class teacher or other approved adult helper.
- Staff check that sites that are pre-selected for pupils’ use are appropriate for their age and maturity.
- Staff are particularly vigilant when pupils are undertaking their own search and will ensure that they are following an agreed search plan.
- Pupils will be taught to use e-mail, social media, Apps and the internet responsibly in order to reduce the risk to themselves and others.
- Members of staff are always aware of the potential for misuse, and are responsible for explaining acceptable use and risks to pupils. This is done at appropriate levels for the age and stage of pupils’ understanding and development.
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with our online service provider.

The experience of many schools has shown these measures to be highly effective, although it is not possible to guarantee that particular types of material will never appear on a school device’s screen.

Pupils are taught to tell a trusted adult immediately if they encounter any material that makes them feel uncomfortable. Should an incident occur in which children are exposed to offensive or upsetting material, the school will respond to the situation quickly and on a number of levels.

- The class teacher and DSL will give appropriate support to the pupils. The pupils’ parents will be informed and given an explanation of the course of action taken.
- The ICT manager will report the URL (address) and content of unsuitable sites to the internet service provider. If it is thought that the material is illegal, after further

consultation with the online service provider, the site will be referred to the Internet Watch Foundation and the Police.

- Responsibility for handling incidents involving pupils will be taken to the Designated Safeguarding Lead and safeguarding procedures will be followed (see the Safeguarding Children and Child Protection Policy).

The pupils' responsibilities

- It is important for pupils to realise that they are expected to play their part in reducing the risk of viewing inappropriate material by obeying the rules of responsible online access. (See appendix 1)
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to online resources. They will also come under the general discipline procedures of the school as outlined in our Behaviour Policy.
- Pupils who are online are expected not to deliberately seek out offensive materials. Should any pupils or staff encounter any such material accidentally, they are expected to report it immediately to the DSL or Headteacher and ICT manager, so that the Service Provider can block further access to the site.
- Pupils must ask permission before accessing the internet and have a clear idea why they are using it.
- Pupils must not access other people's files.
- Computers and tablets, in school, should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the internet. This is to prevent corruption of data and avoid viruses.
- Personal information, such as phone numbers and addresses, must not be given out.
- Uploading and downloading of non-approved software will not be permitted.
- There will be no access to social networking/online gaming or apps such as Tik Tok or YouTube from school equipment.
- Pupils are advised that the use of social networking sites outside of school is inappropriate due to age restrictions.
- Pupils must not share their usernames or passwords with anyone.

Using the internet to enhance learning

- When accessing the internet, pupils will be given clear learning objectives relating to schemes of work, in order to enrich and extend learning activities. Each year group follows a curriculum which is on their long term overviews.
- Access to the internet may be by teacher (or sometimes other adult) demonstration.
- Pupils may work offline to access prepared material, rather than being online.

- Pupils may be given a suitable web page or a single web site to access.
- Pupils will be provided with a list of suitable and relevant web sites, which they will access.
- Older, more experienced pupils may be allowed to undertake their own internet search having agreed a search plan with the class teacher.

Using information from the online

- Pupils will be taught to understand that much of the information available online is intended for an adult audience, is not properly edited and is subject to copyright.
- Pupils will be made aware of the need to validate information from an alternative source wherever possible.
- Pupils will be taught to observe copyright and how to select and record relevant information.
- Pupils will be made aware that the author of web pages or e-mails may not be who they say they are.

Using e-mail

Pupils will learn how to use an e-mail application and be taught e-mail conventions as part of the ICT scheme of work.

Online access and home/school links

- Parents will be informed in the school prospectus that pupils are provided with supervised internet access as part of their lessons and will be kept informed of future developments by letter and newsletter.
- Parents and pupils will be expected to sign a permission form before they begin using the internet to share responsibility with the school.
- Parents are required to inform to the school if they have any objections to their child's work or photographs being published.
- Parents are asked to give permission for their children's photographs to be taken and published on the website.

Expectations of all staff using the online inside and outside school premises

All staff are expected to read the 'Mobile Devices and Acceptable Use Policy, Social Networking Policy, Internet Acceptable Use Policy and the Code of Conduct.

School Website

- The website and Facebook page will be regularly checked to ensure that there is no content that compromises the safety of pupils.
- The publication of pupils' work will be at the decision of the class teacher.

- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual pupils will not be published on the school website without parental permission.
- The school's website will not publish the full names of individuals in a photograph.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

Personal Devices

Pupils may not bring any smart devices to school; this includes mobile phones, smart glasses, smart watches, cameras or other recording devices. They may not use their own technology such as phones, iPads (or other tablets) laptops, smart watches, cameras, glasses or other mobile devices in school.

Parents may not use any smart devices in school to record meetings or productions without express permission from the Headteacher. This includes smart phones, glasses, watches, cameras or other recording devices. (see the Mobile Devices Acceptable Use Policy)

Staff must read the Mobile Devices Acceptable Use Policy. Inappropriate use of any device is in direct breach of the school's Mobile Device Acceptable Use Policy and will be subject to Disciplinary Proceedings.

For acceptable use of the internet, please see the Mobile Devices Acceptable Use Policy.

Policy Implementation

- The School Governing Body is responsible for the implementation, review and evaluation of this policy. It will be consulted during the review of this policy.
- This policy is freely available to all staff, parents/carers and service partners. It will form part of staff induction.

This policy will be reviewed in October 2027 or before if procedures change.

It was agreed and adopted by the Governing Body of Leagrave Primary School in October 2026.

This policy will be implemented in October 2026.