Lever Edge Primary Academy

Online Safety Policy

This online safety policy was approved by the Board of Trustees on:	*December 2025*
The implementation of this online safety policy will be monitored by the:	*Senior Leadership Team*
Monitoring will take place at regular intervals:	*As the need arises but at least once a year*
The school will monitor the impact of the policy using:	Logs of reported incidents Monitoring logs of internet activity (including sites visited) Internal monitoring data for network activity
The Board Trustees will receive a report on the implementation of the online safety policy at regular intervals:	*At full Board of Trustees Meeting*
The online safety policy will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*December 2026 then March 2027 – (when final revised curriculum is due to be released)*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Headteacher/ DSL: Mrs Kelly James* *LADO: Ms. Lisa Kelly* *Police*

Contents

1. Aims

Our school is committed to ensuring that all members of the academy community – including pupils, staff, volunteers, trustees, visitors, and parents – can engage with technology safely and responsibly.

This policy aims to:

- Establish clear processes to **ensure the online safety** of all stakeholders.
- Deliver a **proactive and educational approach** to online safety that empowers the school community.
- Outline **mechanisms for identifying, reporting, escalating, and responding to online safety concerns**.
- Support the development of **critical thinking and resilience** in our pupils regarding their online interactions and presence.

The 4 Categories of Online Risk (UKCIS 2023 Update)

Our approach to online safety is based on understanding and mitigating risks across the following four categories:

1. **Content** – Exposure to harmful or inappropriate content, including pornography, self-harm, suicide content, misogyny, racism, fake news, extremism, radicalisation and online hoaxes.
2. **Contact** – Harmful online interactions with others, including grooming, exploitation, radicalisation, harassment, and unwanted pressure from peers.
3. **Conduct** – Negative personal online behaviours such as cyberbullying, sexting, oversharing, and posting/sharing harmful content.
4. **Commerce** – Financial or commercial risks such as scams, phishing, online gambling, microtransactions, and advertising exploitation.

2. Legislation and guidance

This policy is informed by and compliant with the latest safeguarding and online safety guidance, including:

Statutory Guidance

- DfE *Keeping Children Safe in Education (KCSIE) 2025*
- DfE *Teaching Online Safety in Schools*
- DfE *Preventing and Tackling Bullying (including cyberbullying)*
- DfE *Searching, Screening and Confiscation at School (2024)*
- DfE *Relationships, Sex and Health Education (RSHE) Guidance*
- *Education for a Connected World (UKCIS Framework)*

Legislation

- *Children Act 1989 & 2004*
- *Computer Misuse Act 1990*
- *Education Act 1996, 2002, 2011*
- *Freedom of Information Act 2000*
- *Communications Act 2003*
- *Education and Inspections Act 2006*

- *Equality Act 2010*
- *Counter-Terrorism and Security Act 2015*
- *Serious Crimes Act 2015*
- *Data Protection Act 2018 / UK GDPR*

Other Key Guidance

- UKCIS *Sharing nudes and semi-nudes: advice for education settings* (Dec 2020)
- National Cyber Security Centre (NCSC) guidance for education settings
- Childnet, CEOP, Internet Matters, NSPCC, SWGfL, and other key online safety education partners
- *Prevent Duty Guidance*

This policy complies with our funding agreement and Articles of Association and should be read in conjunction with our safeguarding, behaviour, and data protection policies.

3. Roles and responsibilities

3.1 The board of Trustees

The board of trustees has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The board of trustees 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 trustee who oversees online safety is the safeguarding trustee, Mrs Umal.

All trustees 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, 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, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The Headteacher has a duty of care for ensuring the day-to-day safety (including Online) of all members of the school community. The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The role of the Headteacher will include:

- ensuring that all members of the school community understand and acknowledge their responsibilities in the event of a serious online allegation being made (Appendix 3)
- ensuring that all relevant staff receive suitable training to enable them to carry out their safeguarding responsibilities within the remit of the Online Safety Policy
- ensuring that the Online Safety Policy is accessible to the wider School Community (School website)
- meeting at regular intervals with the Computing Lead to ensure the implementation of this policy (as outlined above). Regular subject leader time is allocated to fulfil the role.
- ensuring regular monitoring from the Computing lead

- ensuring there are opportunities to communicate up to date Online Safety information to the wider school community

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Anti-Bullying and Behaviour Policy.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and 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:

- In ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Computing Lead 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 7) 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 (appendix 5 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the board of trustees

This list is not intended to be exhaustive.

3.4 The Computing Lead / Technical Support

The Computing Lead, in conjunction with the Local Authority ICT team 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 live 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 (see appendix 7) 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.

3.5 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 on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 7) 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'
- Following all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations.
- Having a general understanding of how the pupils in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- Being aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

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
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1&2)

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
- Healthy relationships – Disrespect Nobody

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 to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum specifically computing and Jigsaw (PSHE):

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
- **UKCIS "Education for a Connected World 2024"** framework:
- Critical thinking
- Understanding privacy
- Influence of influencers and algorithms
- Digital footprints and permanence
- Gaming risks (voice chat, loot boxes, spending)
- AI-generated content / misinformation

Pupils in **Key Stage 1** will be taught the following criteria regarding safety:

- **Safe and Respectful Use:** They should be taught to use technology safely and respectfully.
- **Privacy:** They must learn to keep personal information private.
- **Seeking Help:** Pupils should be able to identify where to go for help and support if they have concerns regarding content or contact on the internet and other online technologies.

In **Key Stage** 2, the expectations expand to include responsibility and behavioural recognition:

- **Responsible Usage:** Pupils should be taught to use technology safely, respectfully, and responsibly.
- **Behavioural Standards:** They must be able to recognize acceptable and unacceptable behaviour.
- **Reporting Concerns:** Pupils are expected to 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
- Some people online will use information they find online about children to build trust and use this trust to set traps such as a scam or convince the child to share inappropriate images
- 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

The safe use of social media and the internet will also be covered in other subjects where relevant.

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

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Class Dojo. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher/DSL.

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

6. Cyber-bullying

6.1 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 the school behaviour policy.) Cyberbullying can be a criminal offence (Malicious Communications Act 1988)

6.2 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. Pupils are taught to capture evidence safely (e.g., taking a screenshot and reporting, not sharing further)

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. Class teachers and the Computing Lead will discuss cyber-bullying with their classes.

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, trustees 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/leaflets 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 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.

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 pupils' 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*

* 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 will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors 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 in appendices 1 and 2.

8. Cyber Security

The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage

Lever Edge Primary Academy:

- has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- will conduct a cyber risk assessment annually and review each term
- working with the local authority, has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- has an effective backup and restoration plan in place in the event of cyber attacks
- will ensure the school's governance and IT policies reflect the importance of good cyber security
- will ensure staff and trustees receive training on the common cyber security threats and incidents that schools experience
- will ensure the school's education programmes include cyber awareness for pupils
- has a business continuity and incident management plan in place
- has processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

9. The use of Artificial Intelligence (AI) systems at Lever Edge

Lever Edge recognises that Artificial Intelligence (AI) technology is an evolving tool with significant benefits for education, but its use also introduces new considerations for online safety and safeguarding. Therefore, this policy works in conjunction with our standalone **Policy on the use of Artificial Intelligence at Lever Edge Primary Academy**. The safeguarding of all staff and pupils remains our priority, and we are committed to educating our school community on the safe, ethical, and responsible use of AI. All staff and pupils must adhere to the principles of safe AI use, which are summarised below. For a comprehensive understanding of the school's protocols, responsibilities, and specific risk mitigation strategies concerning AI, please refer to the full AI Policy and its appendixes.

Summary of AI Policy Key Requirements at Lever Edge.

- **Safeguarding Focus:** The school prioritises safeguarding and is committed to educating staff and pupils on the safe, ethical, and responsible use of AI. We acknowledge the increased risk for vulnerable pupils and provide appropriate support.
- **Data Protection:** Staff must only use AI tools approved by the school, use school-provided accounts, and ensure compliance with UK GDPR. A core requirement is to **only input anonymised data** and to never input sensitive or personally identifiable information into unvetted third-party AI tools.
- **Prompt Reporting of Incidents:** Any AI-related incident, including misuse, data breaches, or inappropriate outputs, must be reported promptly to relevant internal teams. Our reporting systems are easily accessible for staff, pupils, and parents/carers.
- **Human Oversight:** AI must assist, not replace, human decision-making. Staff must critically evaluate, fact-check, and review all AI-generated content for accuracy before sharing or publishing.
- **Training and Responsibility:** The Designated Safeguarding Lead/Online Safety Lead is expected to have knowledge of AI and its safeguarding implications. All staff must read and understand the policy and report any suspected incidents.

9.1 Key Points of AI and Online Safety

The following is a summary of the AI policy's key points, specifically in reference to online safety at Lever Edge. These points highlight the importance of being aware of online safety, safeguarding, and data protection when using AI.

9.2 Safeguarding and Risk Mitigation

- **Prioritise Safeguarding:** The safeguarding of staff and pupils is at the

forefront of the policy and practice regarding AI use.

- **Education on Safe Use:** Lever Edge is committed to educating staff and pupils on the **safe, ethical, and responsible** use of AI technologies.
- **Risk reduction:** While the school recognises the benefits of AI, it acknowledges that risks exist, and these will be managed through existing policies (including the Online Safety Policy) and by amending them as necessary to address AI-specific risks.
- **Vulnerable Groups:** The school recognises that vulnerable pupils are more likely to be at risk from the misuse of AI and will ensure they are offered appropriate support.
- **Training on Risks:** Staff training will integrate AI-related risks and safeguards into annual safeguarding training and will equip staff to identify, assess, and reduce risks like privacy breaches, biased algorithms, and harmful content.

9.3 Data Protection and Security

- **Responsible Data Handling:** Staff are required to use AI tools responsibly, ensuring the protection of both personal and sensitive data.
- **Anonymisation:** Staff must **only input anonymised data** to avoid the exposure of personally identifiable or sensitive information into third-party AI tools.
- **Compliance:** AI tools used by staff must comply with **UK GDPR and other data protection regulations**.
- **Approved Tools and Accounts:** Only AI technologies **approved by the school** may be used, and staff must always use school-provided AI accounts for work purposes.
- **No Sensitive Information:** Staff must **not input sensitive information** (like internal documents or strategic plans) into third-party AI tools unless explicitly vetted.

9.4 Reporting and Incident Response

- **Prompt Reporting:** AI incidents, which include AI misuse, data breaches, or inappropriate outputs, must be **reported promptly** to the relevant internal teams to mitigate risks.
- **Reporting Systems:** Reporting systems are well promoted, easily understood, and easily accessible for staff, pupils, and parents/carers.
- **Incident Response:** All reports will be dealt with swiftly and sensitively, following sound **safeguarding principles** and the school's existing safeguarding and disciplinary processes.

9.5 Responsibilities

- **Online Safety Lead:** The Designated Safeguarding Person (DSP) / Online Safety Lead has responsibility for online safety and is expected to have knowledge of **AI and its safeguarding implications**.
- **All Staff Duty:** All staff must read and understand the AI policy and associated Acceptable Use Agreements. They have a duty to ensure the school environment is safe and must **report any incidents** and challenge inappropriate behaviour.
- **Parent/Carer Engagement:** Parents and carers will be made aware of how AI is used and will receive guidance on both good practice in its use and the **risks of misuse** that may affect their children's learning or safety.

10. Pupils using mobile devices in school

Pupils are permitted to bring mobile devices into school.

Mobile technology devices used in school will be school owned and might include: tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless

network. The device then has access to the wider internet.

All users should understand that the primary purpose of the use mobile devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

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 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)
- Use 2 factor authentication (2FA) where possible to add an additional layer of security to block unauthorised access when a password has been stolen/hacked.
- Ensure personal data or identifying data of pupils, guardians and staff is only viewed or used outside school when accessed via a password or 2FA
- 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 – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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 Computing Lead.

12. 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 behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. We will also inform parents/carers of incidents of inappropriate online safety behaviour that takes place outside school.

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 staff disciplinary procedures/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.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding 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 pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils 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, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 7.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/pupils
    - parents/carers
    - staff
    - Annual online safety risk assessment to be completed

Outcomes of monitoring to inform safeguarding and curriculum planning.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the board of trustees. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Social Media

The school's use of social media is to promote the ethos of the school. It is the responsibility of all staff to ensure that the content they upload is for professional purposes only, be compliant with the school policies and protect the identity of pupils. Staff and pupils should not post content relating to school matters without prior approval.

16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use
- Use of Artificial Intelligence at Lever Edge Primary Academy

17. Useful Information

17.1 Safeguarding

In the event of a Safeguarding infringement or suspicion, appendix 6 must be followed with consideration of the following:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a computer that will not be used by pupils and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed (except in the case of images of child sexual abuse – see below)
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include: incidents of 'grooming' behaviour the sending of obscene materials to a child adult material which potentially breaches the Obscene Publications Act criminally racist material other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the relevant group for evidence and reference purposes.

17.2 Data Protection

Personal and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Schools are audited regularly regarding how they handle their data, for further information please refer to school Data Protection Policy.

17.3 Communications

When using communication technologies, the school considers the following as good practice:

- The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school
- When accessing emails out of the schools setting, staff will only be able to access their schools' emails using Microsoft Multifactor Authentication app.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

18. Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix 1:

Lever Edge Primary Academy
KS1 Pupil Technology Agreement

Using Technology at School

My Learning with School Devices

- I will look after school computers, laptops and tablets.
- I know my teachers will watch how I use computers and tablets to keep me safe.
- If something is broken or I need help, I will tell a teacher.

My School Accounts

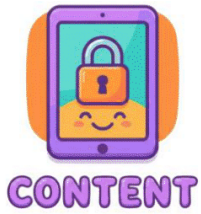
- I will keep my usernames and passwords private.
- I will not use anyone else's login details.
- I will only use the apps and websites my teacher tells me to use.
- I will log off or shut down when I finish.

Being Safe Online and Kind at School

- I will follow our online safety rules and be kind when using technology.
- If something makes me feel worried or upset, I will tell a trusted adult straight away.
- I will use what I've learned about online safety when searching.
- I will not look at, change, or delete other people's work.
- I know that not everything online is true.
- I will not use a camera in school without an adult's permission.
- I will only take pictures of other people with their permission.

Using Technology at Home

Content



- I know that games and websites have age rules to look after me.
- I understand that using apps or sites made for older children or grown-ups isn't safe for me.
- I will tell a trusted adult if something online upsets me.

Conduct

- I know that looking at screens all day is not good for my body or my brain.
- I understand that once I send a message or photo, it can stay there—even if I try to delete it.
- If someone is unkind or unsafe, I won't keep it a secret. I will ask a grown-up to help me use the 'Report' button or contact people who help children (like Childline).
- I will use kind words online and I will 'Think Before I Click.' I will make sure that what I do online is kind to me, my friends, and my school.

Contact

- If I have my own password, I will keep it private.
- I will not share personal information (name, address, phone number, school).
- I know that people online are not always who they say they are.
- I will not share personal information about myself or others with people online.
- I will not take or share photos or videos of myself unless fully dressed.
- I will not take or share photos or videos of others without permission.
- I will be polite and kind when I talk to people online.
- I will check privacy settings with a trusted adult.

Commerce

- I know some websites have things like scams where they will try to steal money from my family.

Pupil Agreement

- I understand that if I make a mistake or forget the rules adults in school will help me learn from what has happened so I can make better choices next time.
- I understand that if I do something online that could upset me or someone else, my trusted adults at home may be told to help me learn from what happened, support me, and make sure I use technology at home safely.

We have read these rules and agree to follow them when:

Lever Edge Primary Academy
KS2 Pupil Technology Agreement

Using Technology at School

My Learning with School Devices

- I will look after school computers, laptops and tablets.
- I know the school will check how I use devices and the internet to keep everyone safe.
- If something is broken or I need help, I will tell a teacher.

My School Accounts

- I will keep my usernames and passwords private.
- I will not use anyone else's login details.
- I will only use the apps and websites my teacher tells me to use.
- I will log off or shut down when I finish.

Being Safe Online and Kind at School

- I will follow our online safety rules.
- If something makes me feel worried or upset, I will tell a trusted adult straight away.
- I will use what I've learned about online safety when searching.
- I will not look at, change, or delete other people's work.
- I know that not everything online is true.
- I will not use a camera in school without an adult's permission.
- I will not take pictures or record videos of other people without their permission.

Using Technology at Home

Content

- I understand some games and websites have age limits to keep me safe.
- I know that using sites meant for older children can put me at risk.
- I will tell a trusted adult if something online upsets me.

Conduct

- I know that spending too much time online is not healthy.
- I understand that things I post online may stay there even if I delete them.
- If something online worries or upsets me, I will tell a trusted adult.
- With an adult's help, I can report unsafe or unkind behaviour online, using the app/social media reporting tool or other online support agencies e.g. CEOP, Childline, Barnardos.
- I will use kind words online and understand that other people may think differently from me.
- I will always think about how my behaviour online could affect me, my friends, and my school.

Contact

- If I have my own password, I will keep it private.
- I will not share personal information (name, address, phone number, school).
- I know that people online are not always who they say they are.
- I will not share personal information about myself or others with people online.
- I will not take or share photos or videos of myself unless fully dressed.
- I will not take or share photos or videos of others without permission.
- I will be polite and kind when I talk to people online.
- I will check privacy settings with a trusted adult.

Commerce

- I know some websites have things that may be unsafe, like scams or gambling.
- With an adult's help, I will report anything online that seems wrong or makes me uncomfortable.

Pupil Agreement

- I understand that if I break these rules at school, I may not be allowed to use school devices.
- If I or my classmates don't follow the rules at home or at school, the adults at school will help us make better choices next time. They will do things to support us, not just to punish us.
- I understand that if I do something online that could upset me, someone else, or the school, the adults who look after me at home will be told. They will help me learn from what happened, support me, and if needed, give consequences to keep everyone safe.

I have read these rules and agree to follow them when:

- I use computers or devices (at school or at home).
- I am online at home and what I do could affect my school or people in it.

_____

Child's Signature

Appendix 2:

Appendix 3: Acceptable use agreement for staff, trustees, volunteers and visitors

Name of staff member/trustee/volunteer/visitor:

addresses, date of birth etc.

- Access personal social networking sites or chat rooms in school.
- Never open attachments to emails unless they come from someone you already know and trust, they could contain viruses or other programs which could destroy all the information and software on your computer
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the school
- Use a personal mobile phone in any way on the school site when pupils are present or in the vicinity neither will I use a personal device to take photos of pupils or staff.
- Use any improper language when communicating online, including in emails or other messaging services
- Have any contact with pupils on social media sites or add them as friends.
- Share anything about the school on personal social accounts (status, news feeds, walls etc.)
- Include any information that identifies pupils, their families, staff or the school when using AI tools.

- I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I have read and understand the above and agree to apply it when using technology in school, as well as the internet and work devices out of school.		
Name:	**Signed:**	**Date:**

Appendix 4:

Dear Parents,

Responsible Use of the Internet and online safety agreement.

As part of our ongoing work to enhance the curriculum and develop pupils' computing skills, Lever Edge Primary Academy provides supervised access to the Internet.

Pupils may use email to communicate with other pupils, research information from reputable sources and use trusted educational websites to develop and apply their skills and knowledge.

We take online safety very seriously. Online safety will be taught and recapped throughout the year ensuring your children know how to stay safe in this ever-changing technological world.

Our Internet access is provided through an education-focused service that uses filtering systems to block inappropriate material. All computer screens are visible in shared areas, and pupils are supervised at all times when online.

Attached is a copy of our **Pupil Technology Agreements**. Please read through these with your child, discuss the importance of using the Internet safely and responsibly, please then read the parent agreement on the next page and return it to school.

Thank you for your support in helping us keep pupils safe online.

If you would like any further information then you could look on our school website www.leveredgeprimaryacademy.co.uk or get in touch via the school office.

Yours sincerely,

K James

Mrs. K James
Head Teacher

Online Safety Parental Agreement

Please sign below to confirm that:

- I understand that my child has signed the Pupil Technology Agreement and has received (or will receive) online safety education to help them use technology and the internet safely both in and out of school.
- I am aware that the school takes all reasonable precautions — including the use of filtering and monitoring systems — to help ensure pupils' safety when accessing the internet and school ICT systems. I also understand that, despite these measures, the school cannot be held responsible for the content my child may come across online, including through mobile technologies.
- I understand that my child's use of the school's ICT systems will be monitored and that the school will contact me if they have any concerns about possible breaches of the Staying Safe Online Agreement.
- I will encourage and support my child to use the internet and digital technologies safely at home, and I will inform the school if I have any concerns about their online safety.
- I will monitor my child's online activity on all devices they use, including the apps, platforms and websites they access.
- I am aware of the age restrictions for social media platforms. I understand that screen-time limits and parental controls can be set on devices, and I will apply these as appropriate for my child's age.

Parent's name	Name of Child / Children
Parent's signature	
Date	

Appendix 5: Online Safety Training Needs – Self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are you aware of good cyber security practice to protect the school from cyber-attacks?	
Do you know how to ensure compliance with UK GDPR when using AI?	
Do you understand the importance of reviewing all AI generated content before sharing or publishing?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 6: Online Safety Flowchart

Online Safety Incident

Support for Bolton Schools

SET – Safeguarding in Education Team:

- Jo Nicholson– Safeguarding in Education Officer – 07917072223
- Natalie France – Safeguarding Education Social Worker – 077258094v90

LADO: Lisa Kelly- 07824541233

Integrated Front Door – 01204 331500

Police protection investigation unit – 0161 856 7949

Community Police - 101

EXIT Team – Exitteam@bolton.gov.uk

Bolton Safeguarding Children's Partnership: Shona Green – 01204 337964

If there is an ICT network issues contact your school ICT provider.

If your provider is Bolton School ICT Unit – contact 01024 332034 or contact@sict.bolton.gov.uk

Appendix 7: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**