Policy title:	Online Safety Policy Green Lane Infant School
Purpose:	To ensure a consistent approach to online safety
Date ratified:	25/09/23
Review date:	This policy will be reviewed annually. Any suggested amendments will be presented to the Governing Board for approval. September 2023
Coordinator/s:	Mrs Kate Lyall (Deputy Headteacher)
Signed:	Mr Jason Williamson (Chair of Governors)

Version control	1.1
Authors:	Kate Lyall (Deputy Headteacher)
Date:	25th September 23
Revision:	

Green Lane Infant School

Online Safety Policy

We believe this policy should be a working document that is fit for purpose, represents the school ethos, enables consistency and quality across the school and is related to the following legislation:

- Obscene Publications Act 1959
- Children Act 1989
- Computer Misuse Act 1990
- Education Act 1996
- Education Act 1997
- Police Act 1997
- Data Protection Act 2018
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Education Act 2003

- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Children and Young Persons Act 2008
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Education Act 2011
- Protection of Freedoms Act 2012
- Counter Terrorism and Security Act 2015

The following documentation is also related to this policy:

- Equality Act 2010: Advice for Schools (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (DfE)
- Prevent Strategy (HM Gov)
- Teaching online safety in school (DfE)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children
- Race Disparity Audit - Summary Findings from the Ethnicity Facts and Figures Website (Cabinet Office)

We believe that all children have the right to be safe in our society. We recognise that we have a duty to ensure robust arrangements are in place for safeguarding and promoting the welfare of children by creating a safe online environment, responding to the ever-changing nature of technology usage.

We acknowledge online safety:

- '....... refers to the act of staying safe online ... and is also commonly known as internet safety, e-safety and cyber safety. It encompasses all technological devices which have access to the internet from PCs and laptops to

smartphones, watches and tablets. Being safe online means individuals are protecting themselves and others from online harms and risks which may jeopardise their personal information, lead to unsafe communications or even affect their mental health and wellbeing.' (National Online Safety)

- '...... is being aware of the nature of the possible threats that anyone could encounter whilst engaging in activity through the internet, these could be security threats, protecting and managing your personal data, online reputation management, and harmful or illegal content.' (South West Grid for Learning)

We work hard to ensure that pupils are safeguarded from potentially harmful and inappropriate online material. We understand that there are many online safeguarding issues that can be categorised into four areas of risk:

Content:	Being exposed to illegal, inappropriate or harmful material 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 child-to-child 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.
Commerce:	Risk such as inappropriate advertising, in-app purchasing, phishing and of financial scams

(Amended from 'Keeping Children Safe in Education')

We believe online safety:

- is an integral part of safeguarding and requires a whole school, curricular approach;
- must follow the school's safeguarding and child protection procedures;
- must be responsive to ever-changing risks;
- will educate our children about the benefits and risks of using technology;
- will provide safeguards and awareness to enable our children to control their online experience.

We ensure all governors undertake online safeguarding training on induction and will attend regular refresher training.

We ensure the IT infrastructure is as safe and secure as is reasonably possible and therefore we have employed an IT service provider who carries out all the online safety measures on our behalf.

We record, classify and track online safety issues using CPOMS in accordance with our safeguarding policy.

We believe that all children, staff and governors have a duty to:

- behave respectfully online and offline;
- use technology for teaching and learning and to prepare for life after school;
- report any concerns or inappropriate behaviour;
- protect each other and the good name of the school;
- promote and model positive online safety behaviour.

We believe the teaching of online safety and its harms must be taught within a whole school approach. This is interwoven through computing lessons, assemblies and class discussions in response to identified concerns. 'It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.' (DfE)

Annually, we also celebrate 'Safer Internet Day' which is celebrated globally in February each year to promote the safe and positive use of digital technology for children and young people.

This policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that are connected with this policy.

Aims:

- To safeguard and promote the welfare of all children as the safety and protection of children is of paramount importance to everyone in this school.
- To ensure arrangements are in place for safeguarding and promoting the welfare of children by creating a safe online environment.
- To create a culture of vigilance and ensure what is in the best interests of all children at all times.
- To ensure compliance with all relevant legislation connected to this policy.
- To share good practice within the school, within Attenborough Learning Trust and with other schools in order to improve this policy.

Responsibility for the Policy and Procedure

Role of the Governing Body

The governing body has:

- ☐ delegated powers and responsibilities to the headteacher to ensure all staff and stakeholders are aware of and comply with this policy;
- ☐ responsibility for ensuring:

- the approval of this policy;
- full compliance with all statutory responsibilities;
- funding is in place to support this policy;
- this policy and all policies are maintained and updated regularly;
- all policies are made available to parents;
- the effective implementation, monitoring and evaluation of this policy undertaken by the governors/directors/sub-committee.

Role of the Headteacher

The headteacher will:

☐ work in conjunction with the senior leadership team to ensure all staff, children and parents are aware of and comply with this policy;

☐ establish a culture of safeguarding where online safety is fully integrated into whole school safeguarding;

☐ undertake training in offline and online safeguarding;

☐ ensure all staff and governors undertake training in offline and online safeguarding;

☐ ensure all staff, children, governors and parents/carers are aware of the procedures to be followed in the event of an online safeguarding incident;

☐ ensure child protection is always put first and data-protection processes support careful and legal sharing of information;

☐ annually report to the governing body on the success and development of this policy;

☐ ensure all staff promote and model positive online safety behaviour in compliance with the school's acceptable use policy

☐ ensure all staff are aware of the potential for serious child protection/safeguarding issues which may arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online conduct
- potential or actual incidents of grooming
- online bullying
- disclosures by children

☐ ensure school staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;

☐ in regard to an online safeguarding issue will liaise with the appropriate safeguarding authority;

☐ log and report all online safety incidents;

☐ ensure a GDPR-compliant framework for storing data is in place;

☐ annually report to the governing body on the success and development of this policy;

Role of the Computing Curriculum Champion

The Computing Curriculum Champion will:

- [ ] ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance;
- [ ] be responsible for reviewing the school online safety policies and documents, including the school's Learner Acceptable Use Agreement (Appendix 1);
- [ ] liaise with IT support personnel;
- [ ] provide guidance and support to all staff;
- [ ] make effective use of relevant research and information to improve this policy;
- [ ] keep up to date with new developments, resources, online safety issues and legislation;
- [ ] organise a series of online safeguarding and child protection workshops to ensure parents/carers are aware of:

  - Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges
  - Working Together to Safeguard Children: A Guide to Inter-agency working to Safeguard and Promote the Welfare of Children
  - the Safeguarding and Child Protection policy
  - all online safeguarding procedures in place;
  - all online safeguarding policies;
  - their role in online safeguarding.

- [ ] ensure good practice is shared throughout the school;
- [ ] monitor the effectiveness of this policy by:

  - monitoring logs of reported incidents
  - speaking with children, staff, parents/carers and governors

- [ ] ensure teaching staff:

  - are aware that RSHE, Computing and Citizenship have the clearest online safety links;
  - identify opportunities to thread online safety through the curriculum and other school activities;
  - monitor what children are doing and consider potential online dangers;
  - supervise and guide children when engaged in online learning activities

- [ ] annually organise Safer Internet Day;
- [ ] provide strategic leadership and direction;
- [ ] provide a curriculum that provides pupils with the essential knowledge they need to be educated citizens in democratic Britain;

- explore ways of improving the curriculum and the way in which we deliver it with a view of ensuring the highest standards of delivery and consistency in children's learning and teaching experiences and opportunities throughout the school;
- provide an environment that is fun, stimulating and challenging to all pupils;
- ensure that teacher and learning equips children with a range of knowledge and skills and a desire for lifelong learning;
- ensure appropriate coverage of the curriculum;
- provide support and advice;
- monitor pupil progress;
- ensure sufficient and up to date resources are in place.

Role of the Data Protection Officer

The Data Protection Officer will:

- have expert knowledge of data protection law and practices;
- inform the school and school personnel about their obligations to comply with the Data Protection Act 2018 laws;
- ensure data management is strengthened and unified;
- monitor compliance with the Data Protection Act 2018;
- manage internal data protection activities;
- ensure risk and impact assessments are conducted in accordance with ICO guidance;
- report data breaches within 72 hours;
- ensure individuals have greater control over their personal data;
- ensure that prior to the processing of an individual's data that:

- the process is in line with ICO guidance;
- the process is transparent;
- the individual will be notified;
- the notification is written in a form that is understandable to children;
- when sharing an individual's data to a third party outside of school that details for the sharing are clearly defined within the notifications

- share an individual's data where it is a legal requirement to provide such information;
- process all written subject access requests from individuals within 40 days of receiving them;
- have in place a formal contract or service level agreement with a chosen data processor who is GDPR compliant;
- ensure the secure disposal of redundant data and IT hardware holding data in compliance with ICO guidance;
- train school personnel;
- conduct audits;

- ☐ be the first point of contact for supervisory authorities and for individuals whose data is processed;
- ☐ keep up to date documentation of all data protection activities;
- ☐ work closely with the headteacher;
- ☐ periodically report to the headteacher and to the governing body;
- ☐ annually report to the governing body on the success and development of this policy;

Role of Staff

Staff will:

- ☐ comply with all aspects of this policy;
- ☐ be fully aware of all online safeguarding policies and procedures;
- ☐ undertake online safeguarding training on induction and when necessary;
- ☐ report all suspected safeguarding concerns and disclosures to the Designated Safeguarding Lead/Deputy Designated Safeguarding Leads;
- ☐ ensure all communications with children and parents/carers are on a professional level;
- ☐ read, understand and sign the Online Safeguarding policy;
- ☐ reinforce online safety messages when teaching;
- ☐ be aware that RSHE and Computing have the clearest online safety links;
- ☐ identify opportunities to thread online safety through the curriculum and other school activities;
- ☐ monitor what children are doing and consider potential online dangers;
- ☐ supervise and guide children when engaged in online learning activities
- ☐ teach all children to:

- keep personal information private;
- report abuse or any form of online bullying;
- use a range of technology safely
- demonstrate appropriate online behaviour;
- consider potential risks and the age-appropriateness of websites

- ☐ create a safe online environment for their children;
- ☐ remind children to follow the acceptable use policy;
- ☐ promote and model positive online safety behaviour

Role of Children

Children will:

- ☐ be aware of and comply with this policy;

☐ be expected to comply with the acceptable use agreement and will be encouraged to adopt safe and responsible use of the internet;

☐ be trained in the importance of:

- adopting good online safety practice;
- reporting abuse, misuse or access to inappropriate materials or any form of online bullying;
- being vigilant in monitoring the content of websites
- recognising and avoiding online safety risks and building their resilience;

☐ be supported:

- in building resilience to radicalisation by providing a safe online environment;

Role of Parents/Carers

Parents/carers will:

☐ be aware of and comply with this policy;

☐ work in partnership with the school;

☐ be made aware that that they play an essential role in the online education of their children;

☐ be expected to support their child to comply with the acceptable use agreement and will be encouraged to adopt safe and responsible use of information technology;

☐ promote and model positive online safety behaviour;

☐ be trained in:

- understanding online safety risks and issues;
- how to monitor their children's online behaviours;
- how to monitor the material that their children may find on the internet

☐ comply with this policy for the benefit of their children;

☐ comply with the Parent Loaned Device Use Agreement (Appendix 2) if borrowing a school device;

☐ be asked to take part in periodic surveys conducted by the school.

Role of the IT Manager

The IT Manager will:

☐ ensure the service provider carries out all online safety measures;

☐ ensure the internet filtering service will be annually reviewed;

☐ ensure access to the internet is designed to protect children and staff by blocking the following content:

- adult content containing sexually explicit images
- violent content containing graphically violent images
- hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- illegal drug taking content relating to the use or promotion of illegal drugs or the misuse or prescription drugs
- criminal content relating to the promotion of criminal and other activities
- gambling content relating to the use of online gambling websites
- non-educational websites such as social networking sites

☐ ensure all users access the internet in accordance with the School's Acceptable Use Policy and will inform the Computing Curriculum Champion and DSLs if at any time they find they have accessed inappropriate internet sites;
☐ ensure the technical infrastructure is secure and not open to misuse or malicious attack;
☐ ensure the online school meets all online safety technical requirements;
☐ keep up to date with online technical information;
☐ promote and model positive online safety behaviour;

Raising Awareness of this Policy

We will raise awareness of this policy via:

☐ School website;
☐ Staff handbook;
☐ Meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops;
☐ School events;
☐ Meetings with staff;
☐ Written communications with home such as notices on Weduc/Seesaw
☐ Annual report to parents;
☐ Headteacher reports to the governing body;

Training

We ensure:

▪ all staff:

☐ have received the appropriate training on all safeguarding policies and procedures undertaken by a registered training provider;
☐ are familiar with the following documentation:

- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children

☐ are aware of the following linked policies:

- All aspects of this policy
- Safeguarding and Child Protection
- Acceptable Use Policy
- Learner Acceptable Use Agreement
- Parent Loaned Device Use Agreement
- Computing Curriculum
- Behaviour Policy

- Anti-bullying
- Remote Learning
- School Website
- Staff Code of Conduct
- Inclusion
- Photograph Policy

- the content of all training is correct, delivered well and engages staff as we believe that the more engaging training is, the better the outcomes that we need to measure;
- that we have in place evidence for all staff that:

☐ highlights the knowledge gaps in the training;
☐ shows how those knowledge gaps were corrected

- all staff understand and undertake their role in safeguarding and child protection effectively.

Monitoring the Implementation and Effectiveness of the Policy

The practical application of this policy will be reviewed annually or when the need arises by the Curriculum Champion, the Headteacher and the safeguarding governor.

Linked Policies

☐ Safeguarding and Child Protection
☐ Acceptable Use Policy
☐ Learner Acceptable Use Agreement
☐ Parent Loaned Device Use Agreement
☐ Behaviour Policy

- ☐ School Website
- ☐ Prevent Duty - Dealing with Extremism and Radicalisation
- ☐ Dealing with Sexual Harassment and Sexual Violence
- ☐ Computing Curriculum
- ☐ Anti-bullying
- ☐ Remote Learning
- ☐ Staff Code of Conduct
- ☐ Photograph Policy

We believe this policy:

- ☐ has been reviewed thoroughly by the safeguarding governor and the Designated Safeguarding Lead has been questioned on it to make sure it stands up to scrutiny;
- ☐ flows and is easy to follow;
- ☐ is an essential part of the school;
- ☐ supports staff in managing certain situations;
- ☐ forms an important framework that will ensure consistency in applying values and principles throughout the establishment;
- ☐ provides guidance, consistency, accountability, efficiency, and clarity on how the school operates;
- ☐ provides a roadmap for day-to-day operations;
  ensures compliance with laws and regulations, gives guidance for decision-making, and streamlining internal processes;
- ☐ is designed to influence and determine all major decisions, actions and all activities taking place within the boundaries set by them;
- ☐ stems from the school's vision and objectives which are formed in strategic management meetings;
- ☐ has been received by all school personnel via appropriate safeguarding training;
- ☐ is provided to all staff and can be found in the policy folder on the server.

Appendix 1

Green Lane Infant School – Acceptable Use Agreement

Learner Acceptable Use Agreement
- This is how we stay safe when we use technology including computers:
- I will only use activities and apps that an adult has told or allowed me to use.
- I will keep passwords and personal information private.
- I will stop using the computer/tablet if someone is talking to me.
- I will ask permission before I take or share someone's photograph.
- I will take care of computers/tablets and other equipment, holding them carefully.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something on the screen that makes me worried, scared or sad.
- I know that if I break the rules I might not be allowed to use a computer/tablet.

Appendix 2

Green Lane Infant School – Parent/Carer
Loaned Device Use Agreement

Digital technologies have become integral to the lives of children, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that children will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of children with regard to their on-line behaviour, ensuring that loaned devices are used in accordance with the acceptable use agreement.
- that loaned devices are returned to the school as requested.

The school is loaning this device to ensure that children have good access to digital technologies to enhance their learning and will, in return, expect children to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that you are aware of the school's expectations of your child(ren). Please share these rules with your child(ren).

Parents/carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work and to agree to use the loaned device in accordance with the acceptable use agreement.

Permission Form

Parent/Carer's Name: ....
Child/ren Name(s) and Classes: ....
Equipment Type: iPad
Serial:

As the parent/carer of the above child(ren), I accept the terms of the acceptable use policy and agree to return the loaned device at the time requested by the school.
I understand that this is for student use only.
I understand that my child(ren) has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that I need to ensure that appropriate filtering systems are in place. I understand that the school cannot be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child(ren)'s activity on the systems may be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will ensure my child(ren) adopts safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child(ren)'s online safety.

The equipment may require servicing/updating which will mean that it is unavailable for use at some points, arranged in advance, throughout the academic year.

Any new applications, or software must be authorised centrally by the school. New mandatory apps will be installed directly onto the home screen.

Signed: .... Date: ....

....

Please sign one copy and return this to the school office. Please keep one copy for your records.

Learner Acceptable Use Agreement

This is how we stay safe when we use technology including computers:
- I will only use activities and apps that an adult has told or allowed me to use.
- I will keep passwords and personal information private.
- I will stop using the computer/tablet if someone is talking to me.
- I will ask permission before I take or share someone's photograph.
- I will take care of computers/tablets and other equipment, holding them carefully.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something on the screen that makes me worried, scared or sad.
- I know that if I break the rules I might not be allowed to use a computer/tablet.

Further information for parents/carers about online safety can be found here:
https://saferinternet.org.uk/guide-and-resource/parents-and-carers
https://www.thinkuknow.co.uk/parents/