Online safety policy

Leasingham St. Andrew’s Primary School

Approved by:	Governing Body	**Date:** December 2021
Last reviewed on:		
Next review due by:	December 2023	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Safeguarding is a serious matter. At Leasingham St Andrew's we use technology and the internet extensively across all areas of the curriculum. Online safeguarding is an area that is constantly evolving. New technologies inspire children and whilst the internet is a great resource, it is important that children are protected from the risks they may encounter. This policy aims to address roles and responsibilities as well as identifying potential risks when using the internet in and outside of school.

We believe that the key to developing safe and responsible behaviours online, not only for the pupils but everyone within our school community lies in effective educations. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school. We believe that we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Maintained schools and academies that follow the National Curriculum insert:

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

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

The governing board 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 governor who oversees online safety is Nick Johnson.

All governors 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 2)
- 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 is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and DDSL 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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with ICT manager (ARK) 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 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 4 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 headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

At Leasingham St. Andrew's Ark ICT Solutions is the ICT Manager.

The ICT manager 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 during Governors meetings at the resources committee.
- 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 5) 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged 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'

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 (appendices 1)

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 and guest wifi policy. (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

Primary schools insert:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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, twitter and newsletters. 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 and/or the 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.)

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.

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. Each class will discuss cyber-bullying as part of the PSHE curriculum following 'Jigsaw'/ Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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.

7. Acceptable use of the internet in school

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

Pupils may bring mobile devices into school but are not permitted to use them at any time within the school grounds.

If pupils bring a mobile device into school, it must be first agreed by the Headteacher or Class Teachers. The device will be kept by the class teacher for the day and returned at the end of the day.

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

9. 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)
- Ensuring that two factor authentication is set up with Senso monitoring software.
- 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 2.

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 Headteacher and then the ICT Manager (ARK)

10. 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.

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 acceptable use and staff code of conduct policies.

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.

11. 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 DDSL 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.

Governors 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed every year by the Computing Subject Leader (Amy Curt). At every review, the policy will be shared with the governing board. 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.

13. 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 policy
- Guest Wifi Policy
- Remote Learning Policy
- Microsoft Teams Policy
- Computing Policy.

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Rules for Responsible Internet Use

Our school uses the internet to help you with your learning. The following rules need to be read, understood, and signed to keep you safe.

Using the laptops/Ipads

- I will only access the school network with my own login.
- I will not try to access files in other people's folders.
- I will close all programs and log out before leaving the computer.
- I will ensure that any external drives that I bring in from outside school have been checked before using them in school.
- I will take care of school equipment.

Using the internet

- I will ask permission from a teacher before using the internet.
- I will only search the internet in ways my teacher has approved.
- I will check who owns an image I may want to use.
- I will minimise the webpage if I find any unpleasant material and report it to my teacher.
- I understand that the school may check my computer files and monitor my internet browsing.

Using Email/messaging/forums

- I will not give my full name, date of birth, home address or telephone number on any website.
- I will not share anyone else's personal information online.
- I will not use the internet to meet someone outside of school hours.
- I will ask permission from a teacher before sending messages.
- Messages I send will be polite and responsible.
- I will immediately report any unpleasant message sent to me.

Signed ___________ Date___________

As the parent/guardian of _______________ I acknowledge that I have read the acceptable use policy on pupil use of school ICT equipment and the internet. I have discussed this with my child and understand that access is designed for educational purposes only. I recognise that the school monitors pupil use through filtering software. I understand that, at times, children will still encounter unpleasant material and in this instance, appropriate action will be taken and such matters will be reported accordingly. I therefore, will not hold the staff, headteacher or governors of Leasingham St. Andrew's School responsible for any such material accessed on the internet.

Signed ___________ Date __________________

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Staff Acceptable Use of Technology

- Do not give anyone access to your login name or password.
- Do not introduce removable media without having it checked for viruses.
- Never use another member of staff's username and password.
- Do not corrupt or interfere with other user's information.
- Do not release personal details including phone numbers.
- Do not reproduce copyright materials without getting permission.
- Do not attempt to visit sites which may be considered inappropriate.
- Use of school internet for business, profit, advertising or political purposes is strictly forbidden.
- Users should log out when their session has finished.
- Using social media to engage in personal attacks is against the guidelines of professional conduct.
- Staff are responsible for the laptop they have been provided with.
- Your laptop's hard drive is not a storage device for personal materials.
- Emails should not be considered a private medium of communication.
- Do not include offensive or abusive language in your messages.
- Ensure your web activities conform to the normal of moral decency.
- Watch out for accidental access to inappropriate materials and report to the DSL.
- Ensure you have checked your classes GDPR forms to ensure that those who do not wish to be online are not put onto the website/twitter.
- Internet access in the classroom is provided for educational purposes only.
- Please ensure you lock screen access during periods of inactivity.
- Laptops must be secured with two factor authorisation through APP or code lozenge.

Social Media

Many staff and governors have raised issues with the use of Facebook and other social media sites. Whilst we cannot insist on a policy, the advice given includes:

- No staff member should accept a child, past or present as a friend.
- It is inappropriate to accept parents as friends – this can leave staff vulnerable
- Comments made on social media should not include any information about the school, children or staff.
- As a contracted employee of Lincolnshire County Council and General Teaching Council, you should endeavour to uphold an appropriate code of conduct.

Signed ___________

Date ____________

THE USE OF OUR GUEST Wi-Fi

Leasingham St. Andrew's School can provide guests and visitors to the school, upon request at Reception, with access to our 'Wi-Fi' service for access to the Internet.

Access is monitored and filtered to comply with our statutory safeguarding and e-safety obligations. The IT infrastructure may be used by guests to further their education and to enhance their professional activities including teaching, research, administration and management. The school ICT System Policies have been drawn up to protect all parties: the staff, visitors, students and the school.

Access to the Internet will enable visitors to research information and to communicate with other users during their visit here. However, you may inadvertently access material with unsuitable content, therefore it is necessary to have guidelines and systems in place for the protection of: visitors, staff, students and governors.

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited and e-mail sent or received if they are found to contravene any of our policies or are inappropriate or illegal.

Visitors are expected to make responsible and appropriate use of the school's computer network during their stay. It is expected that visitors will comply with strict standards set out below.

Guidelines

These are guidelines to follow to protect personal privacy, acceptable use, fair usage and the integrity of the network.

1. All Internet activity should be appropriate to professional activity or education.
2. Use for personal financial gain, political purposes or advertising is not permitted.
3. Posting anonymous messages, accessing any chat rooms and forwarding chain letters is not permitted.
4. Do not interfere with the operation of the network by attempting to install or distribute illegal software, shareware, or freeware or other data files.
5. Do not violate copyright laws.
6. Do not view, send, or display offensive messages or pictures.
7. Do not share or disclose the password you have been allocated with another person.
8. Do not abuse network capacity and be mindful of the uses you are making of this service.
9. Remember the service is filtered and not all of your apps or the websites you visit or other on-line services which you make use of will work as they do from your normal network connection.
10. We have other restrictions in place regarding the use of cameras on Smartphones, Tablets and other IT Devices – those rules take precedence – nothing here permits the use of cameras where another policy would deny it.
11. Do not attempt to access any folders or files on our network unless they are being loaded from our public website.
12. Be prepared to be held accountable for your actions if the Rules of Appropriate Use are violated.
13. Before leaving the premises, you must disconnect from the Guest Wi-Fi. The password for the Guest Wi-Fi should not be saved on the device.

Summary

Using the Leasingham St. Andrew's IT Systems requires you to log-on to the Guest Wi-Fi. By logging on, you agree to abide by this and other policies that apply during your visit. You accept that logs of any activity may be maintained and that in the event of any inappropriate use may be accessed and produced in evidence of any investigation. Serious misuse may result in prosecution.

Print name: ____________________ Signed: ___________________ Date: ____________________

Appendix 3: 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 there any areas of online safety in which you would like training/further training?	