# Online safety policy

# Lansbury Lawrence Primary School

| | | |
|---|---|---|
| **Approved by:** | Owen O'Regan | **Date:** 14th May 2020 |
| **Next review due by:** | December 2022 | |
| **Presented to:** | Full Governing Board December 2020 | |

# 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

# 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 Department'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.

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

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

# 3. Roles and responsibilities

## 3.1 The Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The CFC Committee will review online safety and monitor records as provided by the designated safeguarding lead (DSL) as a standing order item, and it will also be included in the termly HT Report.

The governor who oversees online safety is Chair of the CFC Committee

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 3)

## 3.2 The head teacher

The head teacher 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 designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- 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 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

**3.4 Computing lead**

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike
- Work closely with the Health and Wellbeing lead to ensure that the Relationships and sex education online safety requirements are met.

### 3.5 The ICT Management Company (Clever ICT)

The ICT management company is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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
- Monitoring the school's ICT systems to ensure that safeguards are continually in place
- React immediately when issues that could weaken online safeguarding arise.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Working with the DSL to ensure 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.

### 3.6 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 (appendix 1)

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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.

### 3.7 Parents

Parents are expected to:

- Notify a member of staff or the head teacher 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 and 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 factsheet - Childnet International

### 3.8 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.

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

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

From September 2020 **all** schools will have to teach: Relationships education and health education in primary schools. This new requirement includes aspects about online safety.

*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*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

# 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. This policy will also be shared with parents.

Online safety will also be covered during parents' workshops which are delivered annually.

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 anti-bullying 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. Class Teachers will discuss cyber-bullying with their classes, and the issue will be addressed during computer lessons and at least one assembly each year.

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, 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 has information available on our website about cyber-bullying so that parents 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 anti-bullying 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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 staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1,2,3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

During school hours, 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. A reasonable amount of personal use is acceptable outside of school hours, however this personal use must not weaken safeguarding, breach the school's code of conduct or bring the school into disrepute in any way.

We retain the right to 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 and online safety rules in appendices 1 and 2.

## 8. Pupils using mobile devices in school

Pupils are not allowed to bring mobile devices into school or on to school activities such as residential visits. In rare circumstances, exceptions can be agreed but only with the explicit consent of the head teacher. Where exceptions have been agreed, all use will be supervised and the mobile devices will be stored by school staff.

*Example 1, a parent wishes to be able to contact a child on the journey home: The parent will need to present a case that demonstrates that this is a rare circumstance, and the head teacher will need to agree. The phone would then be handed to the school office before visiting the classroom and collected at the end of the school day.*

*Example 2, a parent wishes to speak to their child while on a residential trip: The mobile device will be stored by the trip leader and given to the children at an agreed time each day; perhaps after dinner in the evening. They would be used only in an agreed communal area. The mobile devices would be returned to the trip leader as soon as they have been finished with.*

## 9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2, or the school's code of conduct, or bring the school in to disrepute in any way.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

USB devices containing data are not acceptable and all data must remain in the cloud when working off-site.

If staff have any concerns over the security of their device, they must seek advice from the ICT management company, Clever ICT.

## 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 the behaviour policy. 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 staff disciplinary procedures. 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).

The DSL and deputies 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. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-Bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

# Appendix 1: online safety rules for pupils

As part of online safety lessons, each class should design and present their online safety rules. The rules given below are examples. Each class may choose to use these rules, but they should be in the children's own words and supplemented with rules from the children's own learning. The rules should be displayed in the classroom for reference and reinforcement during all online activities.

*I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.*

***I will:***

- *Only use the internet with permission from an adult*
- *keep my password a secret*
- *only visit websites that my teacher has agreed*
- *only click on links that we know what they do*
- *tell an adult if I see anything that makes me uncomfortable*
- *make sure that all of the messages I send show respect*
- *tell an adult if I get a message that upsets me*
- *only email people if my teacher agrees*
- *only use my school email address*
- *never give out passwords or personal information (I will not tell them my name, phone number, anything about where I live, my family or where I go to school)*
- *not load photographs of myself onto the computer*
- *never agree to meet someone I've met online.*

For other useful resources and ideas for display see: https://www.lgfl.net/online-safety/resource-centre

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

| Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors | |
|---|---|
| **Name of staff member/governor/volunteer/visitor:** | |
| When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:<br>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature<br>• Use them in any way which could harm the school's reputation<br>• Use any improper language when communicating online, including in emails or other messaging services<br>• Install any unauthorised software<br>• Share my password with others or log in to the school's network using someone else's details<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>• Share confidential information about the school, its pupils or staff, or other members of the community<br>• Promote private businesses, unless that business is directly related to the school as this would be a taxable use and would need to be declared | |
| During school hours, I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.<br>Any personal internet use will be limited and always be in line with the schools' code of conduct and safeguarding procedures.<br>I agree that the school will monitor the websites I visit.<br>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.<br>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.<br>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## Appendix 3: online safety training needs – self-audit for staff

| Online safety training needs audit | |
|---|---|
| **Name of staff member/volunteer:** | **Date:** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| 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? Please record them here. | |

# Appendix 4: using a school device at home

I understand that:

- I need to sign out with the Office any device I take home and Clever ICT will make sure that this information is recorded on Parago, the school's asset management system.

- Any electronic device assigned to me is to facilitate more efficient and effective work practices and is for this use only. Any significant personal use could be deemed a taxable benefit and would need to be declared to the school and HMRC.

- Access to my device will only be through accounts given to me by the school or by an account approved by the school.
    - Including Apple ID; Google Account; and Microsoft – this list is not exhaustive

- The device and anything stored on it always remains the property of the school and the school can expect the device returned and accessed at any time.

- The acceptable use policy applies at all times including the viewing of inappropriate material, including extremist, pornographic or violent material.

- To safeguard personal data loss, personal and sensitive data should not be stored locally on the device. The device should only access personal data through school approved cloud services such as o365
    - Personal data is information that relates to an identified or identifiable individual.

- If the device is used to take photographs or videos of children, they must be used to fulfill their purpose and deleted at the earliest opportunity.

- If the device is lost, I must report this to the Head Teacher or School Business Manager immediately and follow all steps to safeguard any data. For example:
    - changing any services passwords that may be stored on the device locally
    - executing a remote data wipe, if available.

- I understand that if my device is lost, damaged or becomes inaccessible because of reckless or inappropriate behaviour, it may result in disciplinary action and I may be financially liable.

- If I leave the school, I must return my device before my last day of work. Failure to do so could result in a police report in order to recover the device and could affect future references.

Name:_____

Signed:_____

## Appendix 5 : Lansbury Lawrence Primary School Acceptance Use Agreement Form - Parent/Carer and Pupil

Parent/Guardian/Carer Agreement

The School has agreed that a Chromebook will be loaned to your child. This loan is subject to review on a regular basis and can be withdrawn at any time.

As a parent/carer of a student to whom a Chromebook has been loaned you have read and agreed to the following terms and conditions:

- The equipment provided is the property of Lansbury Lawrence Primary School and is for the sole use of assisting in the delivery of the school curriculum.
- I agree to ensure that:
    - Any user treats the equipment with appropriate care and the Chromebook is maintained in good condition.
    - Any user avoids food and drink near the device.
- I agree to ensure that any user only uses software licensed by the school, authorised by the school.
- The school continues to monitor the device during the loan and it will be screened on return.
- Should any faults occur, I will notify the school as soon as possible. Under no circumstances will I attempt to fix suspected hardware or software faults.

Pupil Agreement:

- I understand that I must use school computers in a responsible way.
- I will be aware of "stranger danger" when I am on-line.
- I will not give any of my own personal information, when I am on-line.
- If I see something that makes me feel sad or upset I will tell an adult I know and trust.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be polite and responsible when I communicate with others.
- I will not try to download programmes or apps.
- I will use only websites / programs / apps that my teacher tells me to use.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

I have read and understand the above and agree to follow the guidelines when:

Name of Pupil: _____ Class: _____

Signed (pupil): _____ Date: _____

Parent/Carers Name _____

Signed _____ Date _____