# Online Safety Policy

# Lansbury Lawrence Primary School

| | | |
|---|---|---|
| **Approved by:** | Full Governing Board | **Date:** 21st March 2023 |
| **Next review due by:** | March 2025 | |

# Contents

# Overview

### 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, antisemitism, 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 scams

# Legislation and guidance

This policy is based on the DfE's statutory safeguarding guidance KCSiE 2022 non-statutory advice to schools. It also reflects (but is not limited to) existing guidance and legislation,

- Teaching online safety in schools
- Preventing and tackling bullying
- Cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Protecting children from radicalisationj
- Education Act 1996
- Education Act 2011
- Education and Inspections Act 2006
- Equality Act 2010

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

# Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

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 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.

# Education and curriculum

At Lansbury Lawrence Primary School, we recognise that online safety and broader digital resilience must be threaded throughout the curriculum and that is why we have adopted the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

## Education children about online safety

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.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

## Cyberbullying

### 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.

### 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 in assemblies. 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 cyberbullying, its impact and ways to support pupils, as part of safeguarding training.

The school also provides information 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.

### Education 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 as appropriate. This policy will also be shared with parents.

Online safety will also be raised with parents as needed in face to face meetings, e.g. Parents' Evening or workshops.

Regular digital device workshops are arranged throughout the school year to train parents on how to manage controls & restrictions for their child's devices using Google Family Link, Apple Family Sharing etc.

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 the headteacher.

## Handling online-safety concerns and incidents

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

## Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Agreement as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

## Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools.

Chromebooks used by the pupils are also protected via Classroom Cloud keyword detection software from Netsupport. This software is installed on school devices only and any keywords or concerning content is reported to the DSL and the Safeguarding Team.

At home, school devices are protected by LGFL HomeProtect.

## Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent). Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

## Device usage

Remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

### Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils/students** are not allowed to bring mobile phones to school.
- **All staff who work directly with children** Staff are allowed to bring their personal phones to school for their own use but will limit such use to non-contact time when pupils are not present. Staff members' personal phones will remain in their bags or cupboards during contact time with pupils.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- Parents are not allowed to take photos and videos during celebrations or events (e.g. Christmas show) but are advised not to share on social media sites. If a class has a 'no photo permission child,' the parents will be informed that they are not allowed to take images or record the event.

### Trips / events away from school

Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

### Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

## 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.*

## 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:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share confidential information about the school, its pupils or staff, or other members of the community
- 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.

Any personal internet use will be limited and always be in line with the schools' code of conduct and safeguarding procedures.

I agree that the school will monitor the websites I visit.

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.

| | |
|---|---|
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

# Appendix 3: 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 4: 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.

<u>Pupil Agreement:</u>

- 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 ______________________________