




The LETTA Trust

Online Safety Policy

Approved & adopted on:	Autumn 2023	To be reviewed:	Autumn 2024
Reviewed by:	Trust Board	Signed:	



Contents

1. Aims and approach	3
2. Legislation and guidance	3
3. Roles and responsibilities	4
4. Educating pupils about online safety	6
5. Educating parents about online safety	7
6. Cyber-bullying	7
7. Acceptable use of the internet in school	9
8. Mobile devices in school	9
9. Staff using work devices outside school	10
10. How the school will respond to issues of misuse	10
11. Training	10
12. Monitoring arrangements	11
13. Links with other policies	11
Appendix 1: acceptable use agreement (pupils,parents or carers)	12
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)	14
Appendix 3: online safety training needs – self-assessment for staff	15



1. Aims and approach:

- To educate the whole school community in its safe use of technology
- To ensure the online safety of pupils, staff, visitors and governors
- To establish clear mechanisms to identify, intervene and manage online safety concerns if they occur

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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the DfE's statutory safeguarding guidance [KCSIE 2022](#) non-statutory advice to schools:

- [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 radicalisation](#)
- [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](#) and complies with our funding agreement and articles of association.



3. Roles and responsibilities

3.1 Trustees and governors

The Trust Board has overall responsibility for monitoring this policy and holding the CEO to account for ensuring that headteachers implement it in LETTA Trust Schools. Members of the LGB will meet regularly with school DSLs and will check online safety logs at this time.

All those in governance will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 2)
- Ensure that online safety is included in safeguarding and related policies and procedures
- Ensure that, where necessary, teaching about online safety is adapted for some pupils with special educational needs and/or disabilities (SEND)
- Ensure that effective cyber security checks and measures are in place

3.2 The headteacher

The headteacher is responsible for ensuring that school staff understand this policy, and that it is being implemented consistently throughout the school. The headteacher will monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL works closely with the IT leader and takes lead responsibility for online safety including filtering and monitoring systems:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- understanding the filtering and monitoring systems and processes in place as explained in paragraph 103 of KCSIE 2023
- 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 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying, including sexual harassment online, are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs) that helps staff understand their expectations, roles and responsibilities around filtering and monitoring. This is explained in paragraph 124 of KCSIE 2023
- Liaising with external services if necessary



- Providing regular reports on online safety in school to the headteacher

This list is not intended to be exhaustive.

3.4 The IT leader

The IT leader 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 the designated safeguarding lead (DSL) understands the filtering and monitoring systems and processes in place
- Ensuring that the school's IT systems are secure and protected against cyber attacks from viruses and malware, and that such cyber security safety mechanisms are updated regularly
- Organising full security checks and monitoring the school's IT systems on a termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying, including sexual harassment online, are dealt with appropriately in line with the school behaviour policy
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND, 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

This list is not intended to be exhaustive.

3.5 All staff and visitors

All staff and visitors are responsible for:

- Reading and understanding this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT 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 (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying, including sexual harassment online, are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.



3.6 Parents

Parents are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendix 1)
- If a child is using a Chromebook at home, parents are responsible for what children are accessing online
- Notify a member of staff of any concerns or queries regarding this policy
- Attend online safety training provided by the school

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre:
<https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International:
<http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>
- Healthy relationships – [Disrespect Nobody](#)

4. Educating pupils about online safety

Pupils are taught about online safety as part of the curriculum.

Key Stage 1:

- 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

Key Stage 2:

- 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 the internet and social media will also be covered in other subjects where relevant and schools use assemblies to raise pupils' awareness of the dangers that can be encountered online.

5. Educating parents about online safety

Schools raise parents' awareness of internet safety in letters or information via our website. If parents have any queries or concerns in relation to online safety, these are addressed in the first instance by the DSL or IT leader.

6. Cyber-bullying

6.1 Definition

Cyber-bullying is bullying that takes place online, e.g. through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional and harming of one person or group by another person or group.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We ensure that pupils know how they can report incidents and are encouraged to do so, including where they are a witness rather than the victim. Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, e.g. personal, social, health and economic (PSHE) education.

All staff 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 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.

When resolving an incident of cyber-bullying, the school follows the processes set out in the anti-bullying policy. The DSL considers whether the incident should be reported to the police if it involves illegal material and works with external services if necessary.

6.3 Examining electronic devices



The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate an electronic device if they have reasonable grounds for suspecting that it:

- Poses a risk to staff or pupils
- Is identified in the school rules as a banned item for which a search can be carried out
- Is evidence in relation to an offence

If the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also do the following before a search:

- Make an assessment of how urgent the search is. If the search is not urgent, they will seek advice from the headteacher or DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation
- Always carry out the search with another staff member present

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy and staff code of conduct

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that has been confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm
- Undermine the safe environment of the school or disrupt teaching
- Commit an offence

When deciding if there is a good reason to erase data or files from a device, the headteacher or DSL will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to anyone
- The pupil and/or the parent refuses to delete the material themselves



If inappropriate material is found on the device, it is up to the headteacher or DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 and 2). Visitors are 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 monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Mobile phones or other personal devices

8.1 Using mobile phones or other personal devices in school

Pupils may bring mobile devices into school but these must be handed in to the school office during the school day.

Staff and visitors may also bring personal devices in. However, they must ensure that these are not used during contact time or while children are present. In addition, they must not take photos or videos of children on their personal devices. The use of personal mobile phones or personal devices is restricted to non-contact time, and to areas of the school where pupils are not present such as the staff room.

There are circumstances in which it may be appropriate for a member of staff to have use of their personal mobile phone during contact time. For instance:

- When emergency contact by their child if necessary
- In the case of acutely ill dependents



The headteacher will decide on a case-by-basis whether to allow for special arrangements. School staff can also use the school office number as a point of emergency contact.

8.2 Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Circumstances may include, but aren't limited to:

- Emergency evacuations such as fire drills
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with the staff code of conduct
- Not use their phones to take photographs or recordings of pupils or anything else which could identify a pupil
- Not give personal phone numbers to parents. If necessary, contact must be made via the school office

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.

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. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT leader.

10. How the school will respond to issues of misuse

Where a pupil misuses a school's IT systems or internet, they 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 IT 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 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 receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- 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

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 DDSLs 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.

Volunteers will receive training appropriate to their role in school. 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 downloaded from CPOMS

This policy will be reviewed annually by the CEO and approved by The Trust Board.



13. Links with other policies:

- Child protection and safeguarding policy
- Whistleblowing policy
- Behaviour and anti-bullying policy
- Staff code of conduct
- Information governance policy
- Complaints procedure
- Remote learning and communication with families
- Outbreak management and remote learning plan

Appendix 1: Acceptable use agreement (pupils, parents or carers)

Acceptable use of the school's IT systems and internet: agreement for pupils, parents and carers

Name of pupil:



When using the school's IT systems and accessing the internet in school, I will:

- Only use the Internet for schoolwork, research and homework
- Always make sure there is a teacher or other member of staff present
- When using the Internet at school make sure that I follow my teacher's instructions
- Surf with a friend or another pupil. Two heads are better than one!
- Be a wise surfer. Never access inappropriate websites, never access social networking sites unless this is allowed as part of a learning activity and never use chat rooms
- Ask "Is it true?" and not assume that information published online or in emails is true
- Keep passwords and login names private
- Log in to the school's network using someone else's details
- Only write to email addresses approved by my teachers or parents
- Check with a teacher before opening attachments in emails or following links in emails
- Be careful what I write and make sure not to write things that could upset and offend others
- Never give out personal information such as address or telephone number online
- Never put others in danger by giving out personal information about them online
- Use CEOP to report any inappropriate online activity or tell an adult if I have a problem
- Ignore negative emails and let my teacher know if I'm sent anything I don't like
- Use any inappropriate language when communicating online, including in emails
- Report Cyber-bullying immediately
- Never arrange to meet anyone offline without adult supervision
- Let a teacher or other member of staff know if I find material which might upset or harm me or others
- Remember that some websites and social media are illegal for Under 13s
- Always respect the privacy of other users' files
- Report anything that breaches these rules immediately to my teacher
- Log off or shut down a computer when I've finished working on it

Mobile phones

Pupils: If I bring a personal mobile phone into school, I will hand it in to the school office during the school day.

Parents: If I bring a personal mobile phone into school, I will keep the phone out of sight and will not use it whilst in the school building.



I understand that the school will monitor the websites I visit at school or when using school equipment.

If I do not understand any part of this Acceptable Use Policy, I will ask a member of staff.

Signed (pupil):

Date:

Parent or carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for bringing a mobile phone to school. I will make sure my child understands these.

Signed (parent or carer):

Date:



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

Acceptable use of the school's IT systems and the internet: agreement for staff, governors, volunteers and visitors

Name:

When using the school's IT 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
- Access social networking sites or chat rooms
- Use 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 unless I am required to do so as part of my job

I will:

- only use the school's IT 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
- 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.
- let the designated safeguarding lead (DSL) and IT leader 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
- always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too
- not use personal devices in the presence of children or use these to take pictures of children

I agree that the school will monitor the websites I visit at work or on a work device.

Signed:

Date:



Appendix 3: Online safety training needs – self-assessment for staff

Online safety training needs audit	
Name:	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 an online safety concern?	
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 IT 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.	



Put in place appropriate filtering and monitoring systems

To consider what's 'appropriate' [filtering and monitoring](#) for your school, you should consider:

- The age range of pupils
- The number of pupils
- How often pupils access the IT system
- The costs associated versus the risks
- Your [Prevent duty risk assessment](#)

Read the [UK Safer Internet Centre's](#) guidance for further details on appropriate filters and monitoring systems.

This is explained in paragraphs 141 to 142 of KCSIE.

The designated safeguarding lead (DSL) is responsible for understanding the filtering and monitoring systems and processes in place. This is explained in paragraph 103 of KCSIE.

Make sure safeguarding training for all staff helps them understand their expectations, roles and responsibilities around filtering and monitoring. This is explained in paragraph 124 of KCSIE.

Your governing board is responsible for making sure that these systems and processes are in place, and to regularly review their effectiveness. Your board also should review the DfE's [filtering and monitoring standards](#) and discuss with your IT staff and service providers to support you to meet those standards. This is explained in paragraph 141 of KCSIE