THE LION WORKS SCHOOL POLICY

Online Safety Policy

Author of policy and position of responsibility: Justine Collinson, Headteacher	**Date policy finalised** September 2024
Approved by: Bruno Davis, CEO	**Date of approval** September 2024
Due to be reviewed: July 2025	**Date of review:**

1. Contents
2. Aims
3. Legislation and Guidance
4. Roles and Responsibilities
5. Educating pupils about online safety
6. Educating parents, carers and guardians about Online Safety
7. Cyber-bullying
8. Acceptable use of the internet in school
9. Students using mobile devices in school
10. Staff using work devices outside school
11. How the school will respond to issues of misuse
12. Training
13. Online Safety Reference
14. Monitoring arrangements
15. Links with other policies

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and members of the school board.
- 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 phones and the use of smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where and when appropriate.

The Four 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

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, KCSIE 2024 and its advice for schools on:

- The Independent School Standards 2014
- 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 students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and Responsibilities

3.1 The School Board

The School Board has responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The School Board will be updated by the Headteacher will supervise the work of the DSL.

All members of the school board 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
- Ensure that the Headteacher leads on online safety is a running and interrelated themes while devising and implementing the school's approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, the Headteacher ensures teaching about safeguarding, including online safety, is adapted for all students to be able to access meaningfully. This is 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. The Headteacher takes lead responsibility for online safety in school and therefore is also responsible for:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT managers and other staff, as necessary, to address any online safety issues or incidents swiftly, diligently and effectively
- Managing all online safety issues and incidents in line with the school's Safeguarding and 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's Positive Behaviour Support Policy
- Updating and ensuring that staff are appropriately trained in online safety
- Liaising with other agencies and/or external services if and when necessary

- Providing regular reports on online safety in school to the CEO and School Board
- Ensuring all staff receive online safety training as part of their safeguarding and child protection training

Details of the school's Designated Safeguarding Lead (DSL) and Deputy/Deputies and their related responsibilities are set out in our Safeguarding policy.

3.3 The ICT Service Provider (outsourced to a local company 'Town and County Communication')

The ICT Service Provider, overseen by the Headteacher, is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems (The School uses SMOOTHWALL), which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content, contact and commerce online whilst at school
- 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 on a termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.4 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, and ensuring that students follow the school's terms on acceptable use
- 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's Positive Behaviour Support 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'

3.5 Parents, carers and guardians

Parents, carers and guardians 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

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

- Child Exploitation and Online Protection Centre – Child Exploitation and Online Protection (CEOP) Centre delivers a multi-agency service dedicated to tackling the exploitation of children
- Childnet – Childnet International's mission is to work in partnership with others around the world to help make the Internet a great and safe place for children.
- CEOP thinkuknow – Find the latest information on the sites you like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it.
- Zipit App – Zipit is a free app for you which is designed to provide you with witty images to send in response to a request for explicit images, and advice on how to stay safe – for Android, Apple and BlackBerry smartphones (and iPod touch).
- NSPCC Online Safety – The NSPCC (National Society for the Prevention of Cruelty to Children) provides E-Safety advice and support in a digital world.

3.6 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.

4. Educating pupils about Online Safety

In line with all of our Statutory Guidance in Education, KCSIE 24 and Relationships and sex education and health education, the teaching of Online Safety will be prioritised and taught through our PSHE/RSE curriculum:

By the **end of secondary school**, students 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, contact and conduct and how to report these
- 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, along with signposting through tutor time and Assemblies and Safer Internet Day.

5. Educating parents, carers and guardians about Online Safety

The school will raise parents'/carers' awareness of internet and online safety regularly and in response to local and national contexts. This will also be shared through communications home, information via our website. 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 harm of one person or group by another person or group, often where the relationship involves an imbalance of power. (See also the School's Positive Behaviour Support Policy)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, 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 tutor groups and discuss in Assemblies and as and when appropriate integrate into the wider curriculum; this includes personal, social, health and economic (PSHE) education, ICT lessons and other subjects where appropriate.

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

The school also signposts 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's Positive Behaviour Support Policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is dealt with in accordance with all relevant guidance and contained as far as possible.

This includes reference to: Pan Dorset Safeguarding Children's Partnership; https://pdscp.co.uk/children-young-people/online-safety/, Child Exploitation and Online Protection: https://www.ceop.police.uk/Safety-Centre/ and When to Call the Police.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so and follow this up with a lessons learned exercise and any additional training if any needs are identified.

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 any electronic device that they have reasonable grounds for suspecting:

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

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Headteacher/DSL
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation and record the incident and inform parents

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have 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, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Headteacher 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.

When deciding if there is a good reason to erase data or files from a device, staff members 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 any person, and/or
- The student and/or the parent refuses to delete the material themselves

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 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 Positive Behaviour Support Policy

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

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and members of the school board are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. These are scanned and stored by the school's Administrator. Visitors will be expected to read and agree to the school's terms which are on the visitor information card at reception, which precludes the use of their mobile phones unless agreed by a member of staff.

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. The school reserves the right to monitor the websites visited by students, staff, volunteers, members of the school board and visitors (where relevant) to ensure they comply with the above.

8. Students using mobile devices in school

Students are allowed to bring mobile telephones into school, but are expected to use these responsibly and respectfully. This includes their use only before and after school, breaks and lunchtimes. Any breaches of these conditions will be dealt with individually through the School's Positive Behaviour Support Policy. The natural consequence of inappropriate use of mobile phones may result in a student being disallowed from bringing in their phone, restricted use of their phone

and the introduction of an Acceptable Behaviour Contract. For additional information see the 'Mobile phone and personal device' policy

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 their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- 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 by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use. 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/or the Proprietor / ICT manager.

10. How the school will respond to issues of misuse

Where a student 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 reasonable and 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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider in accordance with national and local guidance 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. These are delivered through Educare. 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 others online through:
- Abusive, harassing, and threatening 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 students can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and Deputy DSL's 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.

Members of the school board 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 Safeguarding Policy.

12. Online Safety Reference:

DfE guidance: Teaching Online Safety in Schools

CEOP (Child Exploitation and Online Protection Centre): Childline: www.ceop.police.uk

Childnet: www.childnet.com

UK Council for Internet Safety

CybermentorsPLUS: www.cybermentorsplus.org

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on Safeguard My School. This policy will be reviewed every year by the Headteacher. At every review, the policy will then be approved by the CEO with guidance and support from the School Board.

14. Links with other policies

This Online Safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Positive Behaviour Support Policy
- Data protection policy and privacy notices
- Complaints Policy and Procedure
- Anti-Bullying policy
- Mobile phone policy