



# **Lumen Academy**

**Embrace   Educate   Empower**

## **E-Safety Policy**

---

**Policy Date: September 2024**

**Review Date: September 2025**

# Document History

Version	Status		Date	Author	Summary Changes
V1			Sep 24	M Sethi	

## Contents:

Aims	2
The 4 key categories of risk	2
Legislation and guidance	2
Roles and responsibilities	3
- The Principal	3
- The Designated Safeguarding Lead	3
- The ICT manager	3
- All staff and volunteers	4
- Parents	4
- Visitors and members of the community	5
Educating pupils about online safety	5
Educating parents about online safety	6
Cyber-bullying	6
- Definition	6
- Preventing and addressing cyber-bullying	6
- Examining electronic devices	7
Acceptable use of the internet in academy	8
Pupils using mobile devices in academy	8
Staff using work devices outside academy	8
How the academy will respond to issues of misuse	9
Training	9
Monitoring arrangements	10
Links with other policies	10
Appendix 2: KS2, KS3, KS4 and KS5 acceptable use agreement (pupils and parents / carers)	11
Appendix 3: Acceptable use agreement (staff, volunteers and visitors)	12
Appendix 4: Online safety training needs – self-audit for staff	13

## Aims

Our academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy 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 Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

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

## Roles and responsibilities

### The Principal

The Principal has overall responsibility for monitoring this policy and holding the staff to account for its implementation. The Principal will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). Principal will:

- Ensure that all staff have read and understand this policy
- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing the academy approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). 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.

### The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy. The DSL takes lead responsibility for online safety in academy, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the academy child protection policy
- 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 academy 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 Principal and/or advisory board.

This list is not intended to be exhaustive.

### The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are

kept safe from potentially harmful and inappropriate content and contact online while at academy, including terrorist and extremist material

- Ensuring that the academy'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 academy's ICT systems on a Fortnightly 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 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy.

This list is not intended to be exhaustive.

### **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 academy's ICT systems and the internet (appendix 3), and ensuring that pupils follow the academy's terms on acceptable use (appendices 1 and 2)
- 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
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### **Parents**

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's ICT systems and internet (appendices 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 resource sheet – Childnet International

## **Visitors and members of the community**

Visitors and members of the community who use the academy'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).

## **Educating pupils about online safety**

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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 people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The safe use of social media and the internet will also be covered in other subjects where relevant. This will include using external agencies to support the delivery of workshops on online safety and supporting students to understand how to use privacy settings and features to protect their personal information.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## **Educating parents about online safety**

The academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (Teams). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings/group sessions. The academy will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the academy (if anyone) their child will be interacting with online
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the Principal.

## **Cyber-bullying**

### **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 1 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 academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, 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 academy also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

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.



## **Examining electronic devices**

The Principal, and the Senior Leadership Team can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the academy 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, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- 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
- 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 DSL and/or the Principal 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 pupil 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 behaviour policy / searches and confiscation policy

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

### **Acceptable use of the internet in academy**

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

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

### **Pupils using mobile devices in academy**

Pupils may bring mobile devices till the main door of the academy, but are not permitted to use them once they are in the academy. They cannot use mobile phones during

- Lessons
- Reflection time
- Activity time before or after scheduled time, or any other activities organised by the academy
- Any use of mobile devices in academy by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).
- Any breach of the acceptable use agreement by a pupil may trigger disciplinary action, which may result in the confiscation of their device.

### **Staff using work devices outside academy**

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 academy's terms of acceptable use, as set out in appendix 3.
- 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 Principal.

## **How the academy will respond to issues of misuse**

Where a pupil misuses the academy's ICT systems or internet, an action will be taken against the user. 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 academy'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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## **Training**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

- 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 up the risks
  - 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 deputy DSL 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 appropriate training and updates, if applicable.
- More information about safeguarding training is set out in our child protection and safeguarding policy.

### **Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every year by the DSL. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

### **Links with other policies**

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Staff disciplinary procedures
- Data protection policy
- Complaints policy

**Appendix 1: KS2, KS3,KS4 and KS5 acceptable use agreement (pupils and parents/carers)**

**ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS**

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.  
When I use the academy's ICT systems (like computers) and get onto the internet in academy I will:

- Always use the academy's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a member of staff is present, or with an responsible adults permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or responsible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher/mentor has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher/mentor.
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the academy's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

**If I bring a personal mobile phone or other personal electronic device into school:**

- I will hand it in to Reception
- I will not use it during lessons, reflection/ group time, clubs or other activities organised by the academy, without a teacher's permission
- I agree that the academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

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

Signed (parent/carer):

Date:

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

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

Name of staff member/volunteer/visitor:

#### **When using the academy's ICT systems and accessing the internet in the academy, or outside academy on a work device (if applicable), I will not:**

Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)

Use them in any way which could harm the academy's reputation

Access social networking sites or chat rooms

Use any improper language when communicating online, including in emails or other messaging services

Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network

Share my password with others or log in to the academy's network using someone else's details

Take photographs of pupils without checking with teachers first

Share confidential information about the academy, its pupils or staff, or other members of the community

#### **Access, modify or share data**

I'm not authorised to access, modify or share

Promote private businesses, unless that business is directly related to the academy

I will only use the academy's ICT systems and access the internet in academy, or outside academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside academy, and keep all data securely stored in accordance with this policy and the academy'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 academy'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:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in academy?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the academy's acceptable use agreement for staff, volunteers and visitors?	
Are you familiar with the academy's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the academy's ICT systems?	
Are you familiar with the academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Reviewed By:

Monika Sethi

September 2024

Next Review Date:

September 2025

Approved by Director:

14<sup>th</sup> September 2024

Signed:

A handwritten signature in black ink, appearing to be 'Monika Sethi', written in a cursive style.

Monika Sethi  
Principal and Director