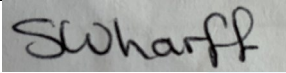


## Online Safety Policy

|                              |                                                                                      |
|------------------------------|--------------------------------------------------------------------------------------|
| Monitoring Responsibility    | Chief Education Officer                                                              |
| Next Review Date             | July 2027                                                                            |
| Approval Body                | Curriculum and Standards                                                             |
| Date Ratified                | 20 July 2026                                                                         |
| Chair of Committee Signature |  |

## 1. Introduction

This Online Safety Policy outlines the commitment of to safeguard members of our school community online in accordance with statutory guidance and best practice.

Each Voyage Academy recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and trustees will be supported to use internet, mobile and digital technologies safely.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

This policy has due regard to the related statutory legislation and guidance including, but not limited to, the following:

- Keeping Children Safe in Education September 2026
- Prevent Duty 2023
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (March 2024)
- Computer Misuse Act 1990
- The Data Protection Act 2018
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- The Protection of Children Act 1978
- Criminal Justice Act 1988
- Public Order Act 1986
- Sexual Offences Act 2003
- The Education and Inspections Act 2006
- The School Information Regulations 2012
- Serious Crime Act 2015
- Criminal Justice and Courts Act 2015
- Online Safety Act 2023

The Children's Wellbeing and Schools Act 2026

This document forms part of our integrated safeguarding portfolio and should be read alongside:

- Voyage Education Partnership: Trust Safeguarding & Child Protection Policy;
- Voyage Education Partnership: Policy and Procedure for allegations and concerns raised in relation to staff, supply staff, contractors and volunteers
- Voyage Education Partnership: Staff Code of Conduct
- Voyage Education Partnership: Prevent Policy

- Voyage Education Partnership: Acceptable Use Policy

## 2. Scope of policy

The policy applies to:

- Pupils
- All Trust staff including all staff based within academies
- Trustees
- Parents/carers
- Peripatetic teachers/coaches, supply teachers, student teachers
- Visitors
- Volunteers

KCSIE 2026 describes online safety risks across four broad areas:

- **Content:** - being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,
- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: 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:** behaviour that increases likelihood of harm for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- **Commerce:** risks such as gambling, inappropriate advertising, phishing and financial scams

Schools in England are subject to increased scrutiny of online safety through inspection, and the Counter Terrorism and Security Act 2015 requires schools to protect learners from terrorist and extremist material online.

## 3. Roles and Responsibilities

### 3.1 Headteacher and senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL/OSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring

- ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Establish a nominated SLT Lead to work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded

The headteacher, have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.

Organisations that are hiring space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

### **3.2 The DSL will:**

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.
- With the nominated SLT Lead and the IT provider lead the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for learners with SEND.

An Online Safety Lead (OSL) may support delivery; the DSL retains lead responsibility.

#### **Online Safety Lead (OSL)**

The OSL will:

- Lead the Online Safety Group and support the DSL day to day.
- Lead development and review of online safety documentation.
- Coordinate awareness, staff confidence and reporting readiness through appropriate training
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.

- Maintain current knowledge of risks across content, contact, conduct and commerce.

Curriculum Leads through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day.

### **3.3 Teaching and Support Staff**

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy and all policies relating to Technical Security and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.

### **3.4 Learners**

Learners will:

- Follow the Learner AUA and Online Safety Policy (including personal devices where permitted).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the Online Safety Policy and share the learner AUA (with local decisions on acknowledgement).
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

### **3.5 The Trust is responsible for:**

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- Review the effectiveness of filtering and monitoring systems annually in conjunction with the DSL
- completing actions following concerns or checks to systems
- In conjunction with the school reviewing the effectiveness of our provision, making sure that processes are in place so that incidents are urgently picked up, acted on and outcomes are recorded

## **4. Cybercrime**

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded
- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing.

It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests. Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs

on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Additional advice can be found at: Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre - NCSC.GOV.UK. D

## On-Line Safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole academy approach to online safety empowers (Insert Academy Name) to protect and educate pupils, students, and staff and families in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. Our Academy ensures that our school devices and network has appropriate filtering and monitoring systems in place supported by our Designated Safeguarding Lead and Trust IT Team to ensure the safe use of our IT and smart technology.

Our Academy recognises that many children have unlimited and unrestricted access to the internet via mobile phone networks (eg 3G, 4G, 5G). This access means some children whilst at school, could sexually harass, bully and control others via their mobile phone and smart technology, share indecent images consensually and non-consensually (often in large chat groups) and view or share pornography and other harmful content.

## 5. Use of Mobile Phones

The Trust has considered the DFE guidance on the use of mobile phones in school. Each of the Trust Academies manage the use of mobile phones in line with this guidance and their own context and is detailed in the Academy Specific Behaviour Policy.

## 6. Curriculum

All Trust Academies ensure online safety is a key feature within the curriculum and our safeguarding of children. Being safe online is well considered within all long-term planning and is reflected in our Academy (please see KCSIE para 134- 151, Trust online safety policy and Trust acceptable use policy and Academy Behaviour policy)

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both within the classroom outside the curriculum, and making the most of unexpected learning opportunities as they arise.

## 7. Reporting and responding

### 7.1 Reporting Concerns

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online or anonymous reporting tools (e.g., Whisper), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual image

### 7.2 Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
  - o Child sexual abuse material (CSAM)
  - o Non-consensual or self-generated images
  - o Grooming, exploitation, or sexual harassment
  - o Terrorism or extremism
  - o Hate crime, fraud, extortion, stalking
  - o Cyber offences under the Computer Misuse Act
  - o Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.

- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

### **7.3 Recording and Monitoring**

The school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- The Trust Safeguarding Lead will provide anonymised summaries of trends and learning to:

Trust Board

Chief Education Officer

## **8. Use of Artificial Intelligence (AI)**

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

## **9. Equal Opportunities**

Voyage Education Partnership is committed to a policy of celebrating diversity, promoting equality of opportunity, providing an inclusive workplace, and eliminating any unfair treatment or unlawful discrimination. This overriding objective applies to all policies and procedures relating to staff and pupils. The Trust will always comply with the requirements of the Equality Act 2010 and associated guidance produced by the Department for Education.

## Appendix A – academy specific information

*Insert academy logo*

**All** breaches of this policy should be reported to the **Academy E-Safety Officer**.

**All breaches of this policy that may have put a child at risk** must also be reported to the **DSL**.

|                               |  |
|-------------------------------|--|
| Academy DSL                   |  |
| Academy Online Safety Officer |  |

The DSL and Online Safety Officer of the academy is responsible for:

- Ensuring there is a holistic approach to OnlineSafety in order to safeguard all learners.
- Ensuring all staff are aware that if a child is at risk of harm then the DSL is notified immediately in line with the Welfare Concerns Pathway.
- Ensuring staff recognise the role of Online Safety in relation to the PREVENT Duty
- Ensuring they understand the filtering and monitoring processes are in place and ensure that staff have the knowledge and ability to report any concerns.
- This includes overseeing and acting on:
  - Filtering and monitoring reports
  - Safeguarding concerns
  - Regularly checking filtering and monitoring systems on site
  - Working with Trust IT staff to make sure the IT systems are effective

The Trust is responsible for:

- Providing the filtering and monitoring system that the academy uses. The Voyage Education Partnership provider is Smoothwall
- Documenting what is blocked or allowed, and why

In conjunction with the school reviewing the effectiveness of the IT systems, making sure that processes in place so that incidents are urgently picked up, acted on and outcomes are recorded