Learning Community Trust

KICKSTART ACADEMY

# Online Safety Policy (including AI)

| | |
|---|---|
| **Date** | February 2026 |
| **Version** | 1 |
| **Circulation** | Website |
| **Owner** | Headteacher and DSL |
| **Date approved** | 10 March 2026 |
| **Approved by** | LGB |
| **Review date** | February 2027 |

# Contents

## Executive Summary

This Online Safety Policy sets out how Kickstart Academy protects pupils, staff, visitors and the wider community when using digital technologies, including artificial intelligence (AI). It outlines expectations for safe conduct online, defines responsibilities, and describes how concerns are reported, managed and monitored.

Key Systems
Filtering: Lightspeed
Monitoring: Senso
Recording incidents: CPOMS
Data Protection Lead: Simon Badley (DPO)
Safeguarding Lead (DSL): Sarah Lewis
Online Safety Governor: Mark Austin

Top Expectations
For pupils:
Use school devices safely and responsibly
Never bypass filtering or monitoring
Report concerns immediately

For staff:
Model safe and appropriate online behaviour
Verify AI outputs and supervise any student AI use
Follow the Acceptable Use Policy at all times

For parents/carers:
Support safe online use at home
Follow school expectations regarding devices, images and communication

What's New in 2026

Expanded section on artificial intelligence
Strengthened mobile phone compliance in line with DfE (2024) guidance
Updated filtering and monitoring standards
Annual Online Safety Risk Assessment process

## Aims

Kickstart Academy aims to:

- Protect pupils, staff, volunteers, visitors and governors through clear online safety expectations and procedures.
- Support pupils who may be more vulnerable to online harm due to additional needs or circumstances.
- Educate the whole school community in safe, responsible and respectful use of technology and mobile/smart devices.

- Ensure a consistent system for identifying, reporting, escalating and responding to online concerns.
- Keep abreast of new risks and take reasonable steps to ensure risks are mitigated.
- Keep risks under review on the school 4 Cs risk assessment.

## The 4 Key Categories of Risk

We address the four Cs DfE-defined areas of online risk:

- **Content:** Illegal or harmful material (e.g., pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, hate content).
- **Contact:** Harmful interactions (e.g., grooming for sexual, criminal, financial or other purposes, manipulation, online pressure).
- **Conduct:** Risky or harmful behaviour online (e.g., bullying, sharing explicit images, consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography).
- **Commerce:** Financial exploitation (e.g., scams, gambling, financial scams, phishing). If we feel our pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

## Legislation and guidance

This policy aligns with:

- *Keeping Children Safe in Education*
- *Teaching Online Safety in Schools*
- *Searching, Screening and Confiscation*
- *Preventing and Tackling Bullying*
- *DfE Using AI in education settings: support materials*
- Education Acts 1996/2006/2011 and the Equality Act 2010.

It meets the requirements of our funding agreement and articles of association.

## Roles and responsibilities

### Governors

- Provide strategic oversight of online safety, ensuring the school meets statutory filtering and monitoring standards.
- Receive regular reports from the DSL on incidents, risks and emerging trends, and ensure follow-up actions are completed.
- Ensure all staff receive annual safeguarding and online safety training, plus interim updates where needed.
- Hold school leaders to account for ensuring that online safety is a thread running through safeguarding, curriculum planning, ICT systems and behaviour expectations.

- Identify a named safeguarding governor with responsibility for monitoring online safety specifically. This is **Mark Austin**.

**Headteacher and DSL (Sarah Lewis)**

- Ensure this policy is clearly understood, communicated and implemented across all provisions.
- Collaborate with the Head of IT and Data at Learning Community Trust to ensure systems remain robust and responsive.
- Ensure online safety remains aligned with wider safeguarding, pastoral systems, curriculum and staff development.
- Take ultimate day-to-day responsibility for online safety in the academy.
- Lead on the configuration, oversight and evaluation of filtering and monitoring systems.
- Maintain accurate logs of incidents, carry out annual online safety risk assessments, and report patterns or concerns to leaders and governors.
- Deliver or coordinate staff training, ensuring all staff receive updated guidance at least annually.
- Liaise with police, external agencies or specialist services where online risks, exploitation, or illegal content are identified.
- Ensure all online safety incidents are responded to in line with the school's child protection procedures.

**Head of IT and Data/DSL at Learning Community Trust**

- Maintain secure school ICT systems through robust filtering, monitoring, antivirus and security protections.
- Conduct regular system checks and audits, reviewing filtering and monitoring effectiveness at least annually.
- Support the DSL to respond rapidly to alerts, breaches, inappropriate access attempts or vulnerabilities.
- Work closely with the DSL to ensure technical systems support safeguarding needs.

**All Staff**

- Model safe, respectful and appropriate online behaviour at all times, following the school's **Acceptable Use Policy**.
- Teach and reinforce safe online behaviour through everyday interactions, curriculum content and pastoral conversations.
- Report any concerns, incidents or suspected risks immediately to the DSL.
- Support pupils in understanding online risks, reporting concerns, and making safe choices.
- Ensure that filtering systems are not bypassed unless appropriately authorised for a legitimate educational purpose.

**Parents/Carers & Visitors**

- Follow the school's **Acceptable Use** expectations when using school equipment or being on site.
- Raise concerns promptly with the DSL if they believe a pupil may be at risk online.

- Work in partnership with the school to reinforce safe and responsible online behaviour at home.
- Visitors accessing the school network or devices must agree to and follow the school's usage conditions.

## Educating pupils about online safety

The aim of our approach to online safety is empowerment to protect and educate pupils and staff in their use of technology and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

We will ensure appropriate filtering and monitoring on school/ devices and networks. The filtering programme is Lightspeed and the monitoring programme is Senso.

We will ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety while planning the curriculum, any teacher training, the role and responsibilities of the DSL (and deputies) and any parental engagement.

We embed the teaching of online safety through the AI Literacy curriculum and via Personal Development (PD) lessons involving online safety.
Pupils in KS4 will be taught:
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity,
- How to report a range of concerns.

By the end of secondary school, pupils will know:
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

- 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. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers via the school website. Online safety will also be covered during parents' evenings. The school will let parents/carers 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 school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## Cyber-bullying

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.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyberbullying with their tutor groups. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying via National College, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to

parents/carers so 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 anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will 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.

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 pupils, 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 pupils and staff. If the search is not urgent, they will seek advice from the Headteacher and/or Lead 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 co-operation.

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 DSL / Headteacher / other member of the senior leadership team 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/carer 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 Child Protection and Safeguarding Policy
- Our Behaviour Policy.

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

## Artificial intelligence (AI)

Artificial Intelligence refers to tools or systems that use automated algorithms to generate text, images, predictions or personalised content, including:

- Generative AI (e.g., chatbots, content generators)
- Adaptive learning platforms
- Predictive analytics or behaviour-monitoring systems
- AI features embedded in educational platforms (e.g., Microsoft 365 tools)

AI offers opportunities to improve administration, teaching, CPD, and personalised learning, but also introduces risks including bias, inaccuracy, safeguarding concerns (using deep fakes to bully), and lack of transparency. These are highlighted throughout the DfE leadership toolkit and safety materials.

Kickstart Academy will treat any use of AI to bully pupils in line with our Positive Behaviour, Relationships and Belonging Policy, Anti Bullying Policy and Child on Child Abuse Policy. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Trust.

**Guiding Principles**
**Safety First**
The DfE requires schools to balance opportunities with safeguarding, privacy, and safety considerations—including transparency, bias, data protection, and intellectual property risks.
**Human-in-the-Loop**

All AI outputs must be checked by a human. AI must support, not replace, professional judgment—emphasised across the DfE support materials and policy papers.

**Responsible Adoption**

Any AI adoption must be purposeful, safe, and aligned with school improvement priorities, as recommended in DfE guidance for leaders.

**Safeguarding**

DfE warns that AI introduces safeguarding risks including:

- exposure to misinformation or inappropriate content
- profiling or biased outputs
- over-reliance by pupils
- lack of transparency around how systems work.

Our school therefore requires:

- teacher supervision of any student AI use
- safe-search or restricted AI environments where possible
- immediate reporting of harmful or inappropriate AI outputs.

**Accuracy, Bias and Transparency**

DfE notes that AI systems may be biased and often lack transparency, even to those who built them.

Staff must:

- verify all AI-generated content
- avoid using AI outputs as fact without cross-checking
- challenge stereotypes or biased responses.

**Approved Tools Only**

- Only AI tools approved by **Trust IT**, the **DSL**, and the **DPO** may be used.
- Public-facing AI tools may not be used for any task involving personal data or sensitive content.
- Staff must complete an **AI Risk Assessment** before adopting any new tool.

**Student Use of AI**

Students may:

- use AI for learning activities where appropriate
- use AI only in supervised or restricted environments
- never submit AI-generated work as their own.

Teachers must:

- explicitly teach safe, ethical AI use
- ensure students understand limitations, such as hallucinations and bias.

**Staff Responsibilities**

**All Staff**

All staff must:

- follow data protection rules
- check accuracy of AI outputs
- use AI only for tasks aligned with professional responsibilities
- report concerns or harmful incidents.

**Leaders**
Leaders must:

- plan AI use strategically, as set out in "Using AI in education: support for school and college leaders"
- ensure CPD and support for safe adoption
- consider workload benefits vs. risks.

**Curriculum Integration**
Students will learn:

- how AI works at a basic level
- ethical considerations
- critical evaluation of AI content

Teachers must ensure AI use enhances learning and does not undermine skill development.

## Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Students will sign the Acceptable use of IT form as part of the Welcome Meeting. Staff will sign the Acceptable use of IT form as part of the laptop and device loan agreement from LCT. Visitors will be 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 will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

## Pupils using mobile devices in school

The school follows the 2024 Government Guidance for Mobile Phone use in school. We follow the guidance that mobile phones should be never used, seen or heard. Students are not permitted to have a mobile phone visible on the premises. Handing in Mobile Phones is part of the normal routine set out in the school's Positive Behaviour, Relationships and Belonging Policy.

Any student visibly in possession of a **mobile phone** will have it confiscated. Phones must never be taken into internal or public examinations. When it is suspected that a mobile phone has been used for inappropriate purposes such as cyber bullying etc. the school has the right to read, copy or delete messages. The phone will be confiscated and returned once parents are informed of the issues. (Links to the DFE document "Screening, Searching and Confiscation" guidance).

Students may not use **e-Watches/iPods/Music Players** at school; other than e-Watches for time telling purposes.

Students are not permitted to make reference to the school, staff or students in **social media**, for example TikTok Youtube and Instagram. These examples are not exhaustive. This includes comments, photographs and naming members of Kickstart Academy. Any student found to have posted material online which refers in any way to Kickstart Academy, a full investigation will be carried out and actions taken as appropriate.

## Staff and Visitor Mobile Phone and Electronics Use

We recognise that staff and visitors are likely to bring a mobile phone onto the school site. The expectation for staff is to have their phone is stored away and not left out on display. Staff are not allowed to take photographs of children on their personal electronic devices.

Acceptable mobile phone use information is shared with visitors who are asked to keep their phones stored away. All teaching staff and teaching assistants have a school laptop. These have been built by the Telford and Wrekin ICT department so are set with appropriate filters. Staff have to input their individual login details in order to get into the computer.

A select group of staff (SLT and pastoral staff) have a school provided mobile phone. These have been built by the Telford and Wrekin ICT department. 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 that 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.

## Technical – infrastructure / equipment, filtering and monitoring

**Mobile technology devices** may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then

has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational.

This Online Safety Policy is consistent with and inter-related to other relevant school polices including but not limited to:
• Child Protection and Safeguarding Policy
• Positive Behaviour, Relationships and Belonging Policy
• Anti-Bullying & Child on Child Policy.

Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education curriculum via IT/Computing and PD.

The development of **digital imaging technologies** has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
• When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
• Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press
• In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital video /images.
• Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital video/images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Students must not take, use, share, publish or distribute images of others without their permission.

• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
• Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
• Student's work can only be published with the permission of the student and parents or carers.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school will ensure that:
• It has a Data Protection Policy.
• It has paid the appropriate fee to the Information Commissioner's Office (ICO).
• It has appointed a Data Protection Officer (DPO). The School appointed DPO is: Simon Badley.
• It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
• Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
• The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
• Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
• Data Protection Impact Assessments (DPIA) are carried out.
• It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
• Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
• There are clear and understood data retention policies and routines for the deletion and disposal of data.
• There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
• Consideration has been given to the protection of personal data when accessed using any remote access solutions.
• All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
• All staff receive data handling awareness/data protection training and are made aware of their responsibilities. Staff must ensure that they:
• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
• Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

• Transfer data using encryption and secure password protected devices. When personal data is stored on any portable computer system, memory stick or any other removable media:
- The data must be encrypted and password protected.
-The device must be password protected.
-The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

When using communication technologies, the school considers the following as good practice:
• The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
• Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
• Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official monitored school systems. Personal email addresses, text messaging or social media must not be used for these communications.
• Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Kickstart Academy adopts the Learning community Trust Social Media Policy. Core messages include the protection of students, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment.

Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to staff and the school through:

- Ensuring that personal information is not published
- Training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff ensure that:

- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents are dealt with under school disciplinary procedures

Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

Personal communications which do not refer to or impact upon the school are outside the scope of this policy. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken. The school permits reasonable and appropriate access to private social media sites Monitoring of Public Social Media. As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school. The school will effectively respond to social media comments made by others according to a defined policy or process. The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

## How the school will respond to issues of misuse

Where a pupil 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 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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents that 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, ebulletins 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, threatening, 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.

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 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 deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

## Monitoring arrangements

The school uses Senso to monitor online safety on devices in school. The DSL or relevant staff member dealing with an incident logs behaviour and safeguarding issues related to online safety via CPOMs. The Online Safety Policy will be reviewed every year by the Lead DSL in conjunction with the Subject Leader for IT and the ICT Manager. At every review, the policy will be shared with the governing board. The review 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
- Positive Behaviour, Relationships and Belonging policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy