# Online Safety Policy

# Drew Primary School

| Date and version | Changes |
|---|---|
| Sept 2026 | Policy Update in line with changes to Keeping Children Safe in Education 2026 |

**Contents**

**Contents** **2**
**Introduction** **3**

| | |
|---|---|
| **Purpose** | **3** |
| **What are the key areas of risk?** | **3** |
| **A shared responsibility for online safety** | **4** |
| **Online Safety in the Curriculum** | **4** |
| **Managing Concerns and Incidents** | **4** |
| **Data Protection and Cyber Security** | **5** |
| **Filtering and Monitoring** | **5** |
| **Use of Generative AI** | **6** |
| **Online communication and data storage** | **6** |
| **Digital Images** | **7** |
| **School Website** | **8** |
| **Social Media** | **8** |
| **Device Usage** | **9** |
| **Appendix A – Roles and Responsibilities** | **12** |
| **Appendix B - Current National Online Safeguarding Trends** | **15** |
| **Appendix C - Handling Safeguarding Concerns and Incidents** | **17** |
| **Appendix D: Use of a pupil's own device for a medical or SEND need** | **17** |


## Introduction

Online safety is an integral part of safeguarding and is addressed through a whole-school approach in line with Keeping Children Safe in Education and other statutory guidance.

This policy applies to all members of the Learning in Harmony Trust community who access school systems, networks or devices, whether on-site or remotely, and at any time.

The Designated Safeguarding Lead (DSL) holds lead responsibility for safeguarding and child protection, including online safety and oversight of filtering and monitoring systems. Tasks may be delegated, but accountability remains with the DSL.

This policy is reviewed annually and updated as required in response to safeguarding developments at national or Trust level and is communicated to staff through induction, training and acceptable use policies and engagement.

**Who are the key people in our school?**

| | | |
|---|---|---|
| **Designated Safeguarding Lead (DSL)**<br>(with lead responsibility for filtering and monitoring) | | Jo-Anne Green<br>Dulcie Sharp |
| **Deputy Designated Safeguarding Leads** | | Julie Clancy<br>Clinton Joseph<br>Una Murtagh<br>Aimee Parker<br>Jackie Welton |
| **Lead Governor for Safeguarding and (web filtering)** | | James Bailey |
| **Key curriculum leads** | PSHE Subject Lead | Julie Clancy |
| | Computing Subject Lead | Farhan Hussain |
| **Head of IT**<br>IT Support Partner | | Louise Pragnell<br>Turn It On |

Online safety is a shared responsibility. All members of the Trust community are expected to behave respectfully and safely online and offline. Detailed role-specific responsibilities are set out in Appendix A.

**Purpose**

The key purpose of this policy is to:

- ensure the safe, responsible, and respectful use of technology.
- serve as an integral part of the school's statutory safeguarding duties and risk management;
- set clear expectations and standards of behaviour;
- establish the actions which should be taken in response to a concern or incident.

**What are the key areas of risk?**

The key areas of online safety risk are the four Cs: content; contact; conduct and commerce.

- **Content:** being exposed to illegal, inappropriate, or harmful content e.g. 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; e.g. 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:** online behaviour that increases the likelihood of, or causes, harm e.g. making, sending and receiving explicit images, including those generated using AI and online bullying
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is the responsibility of all staff to understand the above, recognise when a child may be experiencing harm related to the above, and report to the DSL.

Current national online safeguarding trends can be found in Appendix B.

**A shared responsibility for online safety**

Online safety is a shared responsibility which requires both proactive education and professional vigilance. Students are supported through the curriculum and wider school culture to develop the knowledge, skills and confidence needed to manage online risks responsibly. At the same time, staff are trained to recognise indicators of online harm, misuse or exploitation and to maintain an awareness of emerging risks.

All adults working in school have a responsibility to report any concerns, no matter how small, to the Designated Safeguarding Lead (DSL), maintaining an awareness of online safety issues, the key guidance, and modelling safe, responsible and professional behaviours in their own use of technology.

Staff are responsible for the physical monitoring of students' online devices, and should be aware of the DfE standards for filtering and monitoring, playing their part in providing feedback to the DSL about: overblocking; gaps in provision; or students bypassing protections.

All staff should follow the staff Code of Conduct, Acceptable Use Policy and other key policies, including the relevant parts of Keeping Children Safe in Education. Pages 26-28 of the Safeguarding Policy provides further guidance about online safety.

**Online Safety in the Curriculum**

We recognise the importance of preparing students to navigate the online world safely and confidently. Online safety education is delivered through a planned, age-appropriate and sequenced curriculum which:

- aligns with the National Curriculum requirements for PSHE, RSHE and Computing;
- addresses key online safety risks, including misinformation, extremism and AI;
- supports all students, particularly those who are vulnerable; and
- is reinforced across the wider school curriculum and other areas of school life.

We utilise data from our safeguarding reports, filtering logs, monitoring captures, parental complaints and other stakeholder feedback to inform our curriculum, so that we are constantly learning from concerns and being reflexive and responsive to the needs of our children.

We recognise that nationally, children with SEND are less likely to receive effective online safety teaching, but are more at risk of being a victim of harm caused online. Therefore at [school name], we will ensure that we adapt our curriculum and teaching of online safety for all children, especially those with SEND. We will also consider whether specific filtering policies are required for particular children to afford more protection from online harms. We will also consider targeted and individual interventions that children require to protect them from harm and prevent future online harm.

**Managing Concerns and Incidents**

Online safety concerns are managed in line with the Trust's safeguarding procedures and related policies.

We take all reasonable precautions to safeguard students online, but recognise that incidents will occur both inside and outside school. Any suspected online risk or infringement must be reported immediately to the DSL on the same day. The reporting member of staff will ensure that a record is made of the concern, using the online safeguarding portal (CPOMS) where the concern is about a student. Parents/carers will normally be informed, unless doing so could place the child at additional risk, prejudice an investigation or otherwise be contrary to safeguarding advice

As per the Children's Wellbeing and Schools Act (2026), there is now a mandatory duty for teachers to report any concerns of child sexual abuse, which includes sexual abuse that is facilitated by and/or takes place online (including non-contact abuse such as image sharing). Therefore, all staff must report such concerns without delay to the DSL.

Concerns relating to adults are managed in line with the Trust's Managing Allegations of Abuse against Staff policy and Safeguarding Policy. Any concern or allegation about misuse by adults is always referred directly to the Head Teacher, unless the concern is about the Head Teacher. In this case, the concern is referred to the CEO or Deputy CEO, following the Managing Allegations Policy. Staff may also use the NSPCC Whistleblowing Helpline.

When managing a concern, the school will actively seek support from other agencies as needed, including the LADO and Police where staff or students engage in or are subject to behaviour which we consider is particularly concerning or breaks the law. Schools have obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, particularly relating to social media, where extremism and hate speech can be widespread.

There is further guidance in Appendix C 'What to do if…' for managing particular types of incidents.

**Data Protection and Cyber Security**

Everyone within the school is bound by the Trust's data protection and cyber security policies.

It is important to remember that there is a close relationship between data protection and cyber security, and the school's ability to effectively safeguard all students. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe.

**Filtering and Monitoring**

The DSL has lead responsibility for filtering and monitoring and works closely with the Trust's Head of IT to implement the DfE Filtering and Monitoring Standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems;
- review filtering and monitoring provision at least annually;
- block harmful and inappropriate content without unreasonably impacting teaching and learning; and
- have effective monitoring strategies in place that meet their safeguarding needs.

We provide appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times, ensuring that staff are aware of filtering and monitoring systems and play their part in providing feedback about areas of concern, potential for students to bypass systems and any overblocking. Staff can share their concerns

with the DSL and can ask for feedback in line with the regular checks. Technical and safeguarding colleagues work together closely to carry out an annual online safety audit and regular checks, and also to ensure that the school responds to issues.

The DSL carries out termly checks to ensure filtering is operational and functioning as expected, and completes an annual review as part of an online safety audit of the strategy. More details of both documents and results are available on request from the Trust's Head of IT.

Out of hours, our policies are:

- for filtering devices: filtering reports are run and reviewed during school term time working hours with actions implemented by the end of the next working day.
- for monitoring devices: these are reviewed during school term time working hours, with actions implemented by the end of the next working day.

Staff are informed of the systems in place and their responsibilities during induction and start of year safeguarding training, as well as via our AUP and regular training reminders. The DSL and Head Teacher receive monitoring notifications and take any necessary action as a result.

In line with the DfE standards, our schools monitor students when using school-managed devices, connected to the internet. This could include:

- device monitoring using device management software;
- in-person monitoring in the classroom; or
- network monitoring using log files of internet traffic and web access.

Safe Search is enforced on search engines on all school-managed devices and we use SENSO Monitoring as our digital monitoring tool.

While technical tasks may be delegated, accountability for filtering and monitoring remains with the DSL, in line with the Trust Safeguarding Policy.

**Use of Generative AI**

Generative AI (e.g. ChatGPT, Gemini) is rapidly advancing and access becoming more widespread.

Use of AI can pose data risks, so any use must be approved by the Head Teacher (following appropriate GDPR due diligence, supported by the Head of IT) , and staff are not permitted to use student data on AI platforms.

For students, we block the use of generative AI and only allow access to specific sites. We know that what students input and what different tools output cannot be guaranteed as safe, and inappropriate content can be generated, so we carefully monitor output and limit their use in line with DfE guidance.

We follow the DfE's guidance on this, including:

- carefully managing the use of Gen AI to ensure that users and their data are safe.
- staff are only permitted to use pre-approved Gen AI tools, such as Gemini, and when doing so they must not enter data relating to children, staff or the school which is personal or sensitive.
- clear and well communicated approaches to the use of any Gen AI (by staff or pupils), and this is aligned to school values and pedagogical approaches
- talking about the use of these tools – their practical use as well as their ethical pros and cons;
- recognising that exposure to AI on devices at home for some students may be positive or negative (inappropriate data use, misinformation, bullying, deepfakes, nudifying and inappropriate chatbots); and
- using the Behaviour Policy to manage any situation where generative AI has been used to plagiarise or cheat in an exam.

**Online communication and data storage**

Across the trust, all staff and students have access to Google Workspace, and this is linked to a GMail account. We do not use personal email accounts or messaging apps to communicate with students or parents, or with colleagues when relating to sensitive information. In addition to the use of Google, our school uses the School Management Information System (MIS), Arbor, as the primary messaging tool, and parents may also receive communications via Tapestry..

These systems are managed centrally and administered by the school or authorised IT partner. This is for the mutual protection and privacy of all staff, students and parents, supporting safeguarding best-practice, protecting children against abuse, and staff against potential allegations in line with UK data protection legislation. Data protection principles are followed at all times, in line with the Trust Data Protection Policy.

Use of any new platform or app with communication facilities or student-login requirements, storing sensitive data must be consulted on in advance with the Head of IT. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a student) or to the Head Teacher (if by a staff member).

Staff are allowed to use the email system for reasonable personal use, but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or links to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Where devices have multiple accounts for the same app (professional and personal), mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If a private account is used for communication or to store data by mistake, the DSL / Head Teacher / DPO should be informed immediately (the particular circumstances of the incident will determine whose remit this is). An example of this would be having both a personal and professional Google account and uploading photos to the personal Google Photos app in error.

In line with the Code of Conduct and AUP, appropriate behaviour is expected at all times, and systems should not be used to send inappropriate materials or messages which could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school and Trust into disrepute or compromise professionalism.

**Digital Images**

All use of photography and video by schools must be in accordance with the Learning in Harmony Trust Photography Principles, which reflect guidance on protecting images from AI manipulation and abuse.

We recognise that photographs and videos published online can be copied, downloaded and manipulated, including through generative AI to create sexualised or otherwise harmful imagery of children and adults. When publishing images of pupils or staff on school websites, social media or other publicly accessible platforms and marketing materials, we therefore take a safeguarding-first and proportionate approach. This includes considering whether publication of an identifiable or face-on image is necessary; avoiding high-resolution close-up images wherever possible; favouring lower-resolution images, photographs taken from a distance, from behind or over the shoulder, and carefully selected group or activity shots; ensuring images do not disclose unnecessary personal or location information; and removing embedded metadata where appropriate. Images will only be published where the appropriate consent has been obtained and must never be used where doing so could increase the safeguarding risk to an individual child or member of staff. Our school website is configured to prevent right-clicking, which makes it more difficult to save or copy images directly from the website. We keep our use of publicly available imagery under review as technology and associated risks develop.

Detailed expectations for staff, governors and volunteers are set out in the Acceptable Use Policy, which must be read alongside this policy.

When a student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents/carers are able to answer as follows:

- Use of photographs and videos internally to document learning
- Use of photographs and videos in external publications
- Professional photography individual
- Professional photography group

Whenever a photo or video is created, the member of staff taking it will check the latest database before using it for any purpose. Any students shown in public facing materials are never identified with more than their first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the Trust's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. Photos are stored on appropriate systems, in line with the retention schedule of the Trust Data Protection Policy. Any concerns about the nature of images must be reported to the DSL.

Parents and carers are permitted to take photographs and videos during school events, although the school reserves the right to restrict this for safeguarding reasons. When images are taken, adults are reminded about the importance of not sharing images on social media without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. We encourage young people to think about their online reputation and digital footprint, and so we ask adults to be positive role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not). Further information on managing student images and video content is available here.

In terms of learning about online safety, students are encouraged not to post images or videos of others without their permission and to maintain privacy settings. We educate them about posting safely and the risks associated with providing images and other personal information, including how images can be manipulated. We teach them about the need to keep their data secure and what to do if they or a friend are subject to bullying or abuse.

**School Website**

Our school website is hosted by Greenhouse and provides a key public-facing information portal for the school community (both existing and prospective stakeholders). The Trust Media Manager oversees the statutory compliance of all school websites and the Head Teacher delegates day-to-day responsibility of updating the content of the website to appropriate staff.

When staff produce information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited, and material only used with permission; finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, staff should check with the Trust Media Manager.

**Social Media**

Across the Trust, we work on the principle that if our schools do not manage their reputation on social media, someone else will. Online reputation management is about understanding and managing our digital footprint (everything that can be seen or read about the school and Trust online). Few parents will apply for a school place

without first searching for information about the school online, and the Ofsted pre-inspection check includes monitoring what is being said online.

We manage and monitor our social media footprint carefully to know what is being said about our school and the Trust, and to respond to criticism and praise in a responsible manner. The Trust Media Manager is responsible for managing our social media accounts and checking our Google reviews and other mentions online. Although the school has official social media accounts and will respond to general enquiries, we ask parents/carers not to use these channels, especially not when communicating about their children. The school's Management Information System (MIS) and email provide the standard electronic communication channels between home and school.

If parents have a concern about the school, we urge them to contact the school directly and in private to resolve the matter. If an issue cannot be resolved informally, the complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, students and parents, undermining staff morale and the reputation of the school and Trust.

We ask parents to respect age-ratings on social media platforms and not encourage or condone underage use. The school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

We expect all members of our school community to engage respectfully on social media, setting the same standards that would apply face to face. This includes, but is not limited to not making posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate. Staff are reminded that they are obliged not to bring the school or Trust into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing or oversharing online. Staff should never discuss the school or its stakeholders on social media and should recognise that their personal opinions might be attributed to the school, Trust or wider profession. This expectation applies both to public pages and to private posts, e.g. parent chats, pages or groups.

**Device Usage**

Detailed expectations for staff, governors and volunteers are set out in the AUP, which must be read alongside this policy. The AUP reminds those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague.

1. **Personal Devices**

   Students are permitted to bring mobile phones into school if they are walking to/ from home on their own, but they must have written permission from parents. This applies only to Years 5&6: children in younger year groups are not allowed to bring a phone to school. When parents give permission for their child to bring a phone to school, they and their child are agreeing that:

   - The child hands it to their teacher during registration;
   - The child is not allowed to use their phone whilst on school grounds;
   - If the child is found with a phone on them, staff will confiscate it. The phone will be kept safe until a parent is able to collect it from us.

   Any attempt to use a phone during the school day without permission or to take illicit photographs or videos will lead to the appropriate sanctions as set out in our Behaviour Policy and the withdrawal of

mobile privileges. Other personal recording devices such as smart glasses are not permitted in school. It is forbidden to take secret photos, videos or recordings of teachers or students with any device.

Important messages and phone calls to or from parents can be made via the school office, which will also pass on messages from parents to students in emergencies. Our approach to students using mobile phones is in line with the DfE Mobile Phone Guidance.

- **Staff who work directly with children:**
  Staff working directly with children will be asked to leave their personal mobile phone(s) out of sight and turned off or on silent. Personal devices are not to be used in the presence of children, unless they are being used to access two-factor authentication for logging safeguarding or behaviour incidents, or there is an exceptional circumstance and the Head Teacher has given their permission. The same principles apply to wearable technology such as smart glasses, with the ability to record images, which should not be worn in school. Exceptions would be in an emergency situation on a school trip, or in the event of a lockdown-in-vacuation, or evacuation of the school premises.

- **Governors, volunteers and contractors:**
  Personal mobile phones should not be used in the presence of children, should be switched to silent, and never used to take photographs or videos of children whilst in the school. Other personal recording devices such as smart glasses are not permitted in school. It is forbidden to take secret photos, videos or recordings of teachers or students, including remotely, with any device.

- **Parents, carers and other visitors:**
  Parents, carers and visitors to the school are asked to leave their mobile phones in their pockets and turned off or on silent when they are on site. They should ask permission before taking any photos e.g. of displays in corridors or classrooms, and avoid capturing other children. Please see the Digital Images section of this document for more information about filming and photography at school events. Parents are asked not to call students on their mobile phones during the school day; urgent messages can be passed via the school office. We do not allow Apple AirTags or similar devices in school.

**On occasions when Bring your Own Device (BYOD) is allowed, neither staff nor students are allowed to use a personal mobile hotspot in school to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.**

2. **School Devices**

   Staff and students are expected to follow the terms of the AUP for appropriate use and behaviour on school devices, whether on site or at home. School devices must not be used in any way which contravenes the AUP, the Code of Conduct or the school's policies on behaviour.

   Wi-Fi is accessible to staff and students for school-related use. Staff may use the network for limited personal use within the framework of the AUP. All use is monitored.

   School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning as well as appropriate personal use. All usage of devices and platforms may be tracked.

3. **Using devices on educational visits**

   For educational visits, teachers can be issued a school phone which can be used for any authorised or emergency communications with students, parents or the school.

Staff using their personal phone on an educational visit will ensure that the number is hidden to avoid a parent or student having access to a member of staff's private phone number.

If during an educational visit, students are encouraged to connect their device to another organisation's Wi-Fi network, staff must be conscious of the fact that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in school and therefore maintain a level of responsibility for risk assessing and managing such situations.

Parents will be reminded about their child's permitted device use whilst on trips away from school, including that tracking devices such as Airtags are not permitted for the safety of all pupils.

## 4. Searching and Confiscation

Searching, screening and confiscation of devices is carried out in line with DfE guidance. Only authorised staff may carry out searches, and these must always be proportionate and documented.

**Appendix A – Roles and Responsibilities**

As well as the responsibilities for all staff, there are key responsibilities for some specific roles within the school. These are set out below.

**Head Teacher**

**Key Responsibilities:**

- Foster a culture of safeguarding where online safety is fully integrated.
- Oversee and support the activities of the Designated Safeguarding Lead (DSL) and safeguarding team, and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.
- Ensure all staff undergo safeguarding training (including online safety) at induction and with regular updates, and that they agree and adhere to policies and procedures.
- Ensure all governors undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Ensure that online safety education is embedded across the curriculum in line with the statutory guidance.
- Liaise with the DSL on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support the DSL and technical staff as they review protections for students in the home and remote-learning procedures, rules and safeguards.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO and DSL to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure the school website meets statutory requirements.

**Designated Safeguarding Lead (DSL)**

**Key Responsibilities:**

*The DSL can delegate certain online safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education.*

- The DSL should "take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- Ensure an effective whole school approach to online safety as per KCSIE.
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine(s) etc.

- Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to students confused.
- Ensure all staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
    - This must include filtering and monitoring and help them to understand their roles.
    - All staff must read KCSIE Part One. School leaders and those staff who work directly with children should also read Annex A
    - Cascade knowledge of risks and opportunities throughout the organisation.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Work with the Head Teacher and DPO to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and undertake specific Prevent training.
- Receive regular updates about online safety issues and legislation, and be aware of national, local and school trends.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents.
- Communicate regularly with SLT and the safeguarding governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to online tutors, who should be asked to sign the contractor AUP.

**Safeguarding Governor**

**Key Responsibilities**

- Read all of KCSIE to ensure all governors understand their safeguarding responsibilities.
- Have regular strategic reviews with the DSL, which cover online safety, including discussion of the new filtering and monitoring standards.
- Check that all staff have received appropriate safeguarding and child protection (including online) training at induction and that this is updated.
- Ensure online safety is included in safeguarding discussions at LGB meetings.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children in a safeguarding capacity have also read Annex B.
- Ensure that all staff undergo safeguarding and child protection training (including online safety).
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.
- Ensure appropriate filtering and monitoring systems are in place and their effectiveness is regularly reviewed at least once every academic year.

**Network Manager (and Technical Support)**

**Key Responsibilities:**

- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the DfE standards.
- Keep up to date with the Trust's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding leads / online safety lead / data protection officer / LGfL nominated contact / curriculum leads to ensure that Trust and school systems and networks reflect Trust policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc).
- Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with Trust policy.
- Manage the Trust's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.

**Data Protection Officer (DPO)**

**Key Responsibilities:**

- Provide data protection expertise and training and support the Data Protection and Cyber Security Policy and compliance with those and legislation and ensure that the policies conform with each other.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note the retention schedules for safeguarding records and ensure Trust compliance with this.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

**External Groups (e.g. those hiring the premises)**

**Key Responsibilities:**

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the Internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, students or other parents/carers.

**Appendix B - Current National Online Safeguarding Trends**

**Current National Online Safeguarding Trends**

Nationally, some of the latest trends of the past twelve months are outlined below. These are reflected in this policy and the acceptable use agreements we use and seen in the context of the KCSIE 2026:

**1. LGFL SENSO MONITORING**

The following are concerns highlighted through LGfL's partnership with Senso and monitoring data from LGfL schools. Many children are using Gen AI platforms on the school network and/or school devices, and the following have occurred:

- The creation of child sexual abuse material by and of children
- The spread of AI generated hoaxes, misinformation and disinformation. Sometimes these can be so realistic that it is difficult to determine what is true or not. One notable example of this was the sharing of fake information across social media about serious threats of violence in and between schools, which led to children/parents being fearful and some not attending school.
- Children turning to Gen AI platforms for advice – some of which is harmful and extremely worrying, e.g. dieting, relationships, bullying, and advice about self-harm
- Increased use of AI companions and chatbots which mimic human connection and have been seen to lead to AI induced psychosis, overuse, and heightened feelings of loneliness and shame. Tragically, there have also been numerous cases worldwide of children dying by suicide as a result of interactions with such bots.

There have also been numerous concerns related to staff use of Gen AI, including privacy and intellectual property breaches, and an increase in poor quality learning resources created using Gen AI.

Schools must address this, not just in the classroom, but by educating staff, governors, trustees, parents and pupils on safe use of digital technology, both for school and personal use. For guidance and resources, visit genai.lgfl.net.

LGfL Senso monitoring data has also revealed other concerns in schools:

- Children accessing inappropriate online games, dating sites and web chat where there is the risk of seeing adult and violent content and having interactions with strangers.
- The normalisation of violent and racist language between children, much of which doesn't suggest a particular ideology, but which could lead to extremism.

All these issues require a whole school approach to online safeguarding, as there is no quick or simple solution. It requires a combination of strong leadership, clear roles and responsibilities, robust policies and procedures, effective technical systems, highly competent staff who are regularly updated on this fast paced world, effective and regular collaboration with parents, successful digital literacy and online safety teaching and more.

**2. OFCOM'S LATEST RESEARCH**

Ofcom's 'Children and Parents media use and attitudes report' published in 2026 has shown the following:

Internet use is nearly universal, with 99% of 8-17-year-olds going online, and the vast majority of children are using digital technology by the time they start primary school. A critical transition occurs at age 11, where personal mobile phone ownership jumps from 56% to 83%. Schools must also address the rapid adoption of Generative AI, now used by 56% of 8-17-year-olds, primarily for schoolwork (51%). Despite high confidence, a 'digital literacy

gap' exists: 31% of students could not identify a fake social media profile, and 46% believe AI search summaries are "always accurate".

Social pressures remain high, with 70% of students feeling pressure to be popular on social apps. Negative experiences are common; 23% of 8-17 year olds personally experienced "nasty or hurtful" behaviour in the last year, occurring most frequently on social media (47%) and in online games (38%). Vulnerable students, such as those with mental health conditions, are significantly more likely to feel their screen time is "too high" (56%).

Schools are the primary source of online safety information for 49% of parents. While 85% of students recall online safety lessons, only 23% remember being taught how to spot AI-generated content, and 21% recall lessons on identifying advertising. This suggests a need for updated curricula that reflect the evolving risks of AI and commercial influence.

**3. IWF, CSAM CONCERNS**

Data from the IWF in their 2025 annual report highlights the scale of child sexual abuse imagery online. In 2025, the IWF assessed 451,210 reports, confirming that 311,610 contained child sexual abuse material (CSAM).

Schools should be specifically alert to emerging and persistent harms identified by the IWF, which include:

- Sexually coerced extortion (sextortion): Targeted threats against students – teenage boys in particular.
- AI-generated abuse: The use of generative tools to create non-consensual sexual imagery.
- Violence against women and girls (VAWG): A growing trend in digital spaces around violent and misogynistic narratives and language.

**4. "COM NETWORKS"**

A further concern highlighted by the National Crime Agency, is that of the existence of 'Com Networks'. These are networks of predominantly teenage boys, dedicated to inflicting harm and committing a range of criminality both on and offline, including cyber, fraud, extremism, serious violence, and child sexual abuse. The victims of these crimes are typically other children, some as young as 11, who have been coerced into seriously harming or sexually abusing themselves, siblings or pets. These networks are not hidden away in the dark web, but instead on platforms such as Discord, Telegram, Roblox, and Minecraft. Schools can help to protect children from these networks by enforcing effective filtering, training staff to recognise signs of exploitation, supporting parents to understand and mitigate the risks and building a curriculum that teaches students to identify grooming behaviours.

**5. CYBER ATTACKS**

Data from the Department for Science, Innovation and Technology (DSIT) states that 73% of secondary schools and 49% of primary schools identified a cyber breach or attack in the past 12 months (a significant jump from the previous year). Phishing remains the biggest entry point. AI is being used by scammers to generate sophisticated, error-free phishing emails targeting school administration and staff accounts. Schools are encouraged to ensure that they bridge the gap between technical understanding/cyber security policies, and operational understanding and practice.

## Appendix C - Handling Safeguarding Concerns and Incidents

### Online Safety: What To Do If… Guidance

| | |
|---|---|
| **Concern** | An inappropriate website is accessed **unintentionally** by a student or member of staff. |
| **Action** | 1. Play the situation down; don't make it into a drama.<br>2. Report to the Head Teacher and decide whether to inform parents of any students who viewed the site.<br>3. Inform the IT technician and ensure the site is filtered.<br>4. LGfL schools must also report to Atomwide via the LGfL helpdesk. |

| | |
|---|---|
| **Concern** | An inappropriate website is accessed **intentionally** by a student. |
| **Action** | 1. Refer to the Online Safety rules and agreement signed by the student.<br>2. Report to the Head Teacher.<br>3. Agree the appropriate sanctions in line with the school's Behaviour Policy.<br>4. Notify the student's parents/carers.<br>5. Inform the IT technician and ensure the site is filtered (if necessary). |

| | |
|---|---|
| **Concern** | An inappropriate website is accessed **intentionally** by a staff member. |
| **Action** | 1. Ensure all evidence is stored and logged.<br>2. Report to the Head Teacher.<br>3. Refer to the Acceptable Use Agreement that was signed by the staff member, and apply the appropriate disciplinary procedures.<br>4. Notify the Chair of Governors and CEO.<br>5. Inform the IT technician and ensure the site is filtered (if necessary).<br>6. If the material is of an illegal nature, contact the police and follow their advice. |

| | |
|---|---|
| **Concern** | An adult uses school IT equipment inappropriately. |
| **Action** | 1. Ensure you have a colleague with you, do not view the misuse alone.<br>2. Report the misuse immediately to the Head Teacher and ensure that there is no further access to the device. Record all actions taken.<br>3. If the material is offensive but not illegal, the Head Teacher should then:<br>▪ Remove the device to a secure place.<br>▪ Instigate an audit of all IT equipment by the schools IT managed service providers or technical teams to ensure there is no risk of students accessing inappropriate materials in the school.<br>▪ Identify the precise details of the material.<br>▪ Take the appropriate disciplinary action, following the Trust's policy, contacting the LADO as required.<br>▪ Inform TLG of the incident.<br>4. In an extreme case where the material is of an illegal nature:<br>▪ Contact the LADO and the police and follow their advice.<br>▪ If requested, remove the device to a secure place and document what you have done. |

| | |
|---|---|
| **Concern** | An online bullying incident directed at a student, inside or outside of school time. |
| **Action** | 1. Advise the student not to respond to the message.<br>2. Report to the Head Teacher. |

| | |
|---|---|
| | 3. Refer to relevant policies and apply appropriate sanctions.<br>4. Secure and preserve any evidence through screenshots and printouts.<br>5. Notify parents of all the students involved.<br>6. Consider delivering a parent workshop for the school community.<br>7. Inform the police and/or other agencies if necessary. |

| | |
|---|---|
| **Concern** | Malicious or threatening comments are posted online about a member of the school community (including students and staff). |
| **Action** | 1. Report to the Head Teacher.<br>2. Secure and preserve any evidence. Consider sending the evidence to CEOP at https://www.ceop.police.uk/Contact-Us/<br>3. Inform and request the comments be removed if the site is administered externally.<br>4. Endeavour to trace the origin and ask them to remove the comments.<br>5. Inform the police and/or other agencies if necessary.<br>6. Inform TLG and liaise with PLMR for further advice is required. |

| | |
|---|---|
| **Concern** | You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with them. |
| **Action** | 1. Report to the Head Teacher and/or Designated Safeguarding Lead.<br>2. Contact the child's parents/carers.<br>3. Secure and preserve any evidence*.<br>4. Advise the child on how to terminate the communication.<br>5. Contact CEOP at https://www.ceop.police.uk/Contact-Us/<br>6. Inform the police and/or other agencies if necessary.<br>7. Consider delivering an Online Safety workshop for the school community.<br><br>** In cases of sexting, where there are images of children involved, you must confiscate the device and follow the above procedures. Never make or send copies of any images as this in itself is a crime. Further advice is available here.* |

| | |
|---|---|
| **Concern** | You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child. |
| **Action** | 1. Report to the Head Teacher and/or Designated Safeguarding Lead.<br>2. Contact the child's parents/carers.<br>3. Advise the child and parents/carers on appropriate games and content. You may want to use LGfL template letters to inform all or targeted parents.<br>4. If the game is played within the school environment, ensure that the IT technician blocks access to the game.<br>5. Consider the involvement of social services.<br>6. Consider delivering an Online Safety workshop for the school community. |

| | |
|---|---|
| **Concern** | You are aware of social network posts/pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond. |
| **Action** | 1. Report to the Head Teacher.<br>2. Contact the poster or page creator and discuss the issues in person, asking them to remove the post(s).<br>3. Provide staff training and discuss as a staff how to behave when finding such posts and appropriate responses.<br>4. Consider delivering an Online Safety workshop for the school community. |

| | |
|---|---|
| | 5. Inform TLG and liaise with PLMR for further advice is required. |

## Appendix D: Use of a pupil's own device for a medical or SEND need

The Trust's rules on pupil mobile phone use remain in place. A school may agree to an individual exception where a pupil needs to use their own device to manage a medical condition e.g. to track blood sugar or as a communication aid related to Special Educational Needs and Disabilities (SEND). Permission must be based on the pupil's needs and be recorded before the device is used in school.

The school will agree the arrangements with the pupil and their parents or carers, and with relevant health, SEND or other professionals where appropriate. The arrangements must be reflected in the pupil's relevant individual plan, such as their EHCP, communication plan or risk assessment. Staff who support or supervise the pupil must be made aware of the agreed arrangements.

**Individual device agreement**

The school will keep a central record, using Appendix 1, for each approved exception setting out:

- Pupil name
- Reason for the exception
- Approved device, including any necessary identifying details
- When, where and how the device may be used
- Where the device will be kept when it is not in use
- Network arrangements, including use of LGfL2-GUEST
- Applications and functions the pupil may access
- How use will be supervised and by whom
- Confirmation that the use of the device is recorded in the pupil's individual plan or risk assessment
- Date agreed and people involved
- Review date

The device may be used only in accordance with the recorded agreement. Any proposed change to the device, its functions or how it is used must be discussed with the school so that the agreement and relevant individual plan can be updated. The school will review the arrangement by the recorded review date, or sooner if the pupil's needs or circumstances change.

## Use of a pupil's own mobile device for a medical or SEND need

| | |
|---|---|
| School name | |
| Pupil name | |
| Reason for the exception to the Trust's own mobile device rule | |
| Approved device, including any necessary identifying details | |
| When, where and how the device may be used | |
| Where the device will be kept when it is not in use | |
| Network arrangements, including use of **LGfL2-GUEST** | |
| Applications and functions the pupil may access | |
| How use will be supervised and by whom | |
| Is use of the device recorded in the pupil's individual plan or risk assessment | |
| People involved in this agreement | |
| Date agreed | |
| Review date | |