

Online Safety Policy
2026-2027

Contents

1. Introduction	5
2. Overview	7
3. Roles and responsibilities	8
4. Education and curriculum	8
5. Handling safeguarding concerns and incidents	10
6. CCTV	15
7. Extremism	15
8. Data protection and cyber security	16
9. Appropriate filtering and monitoring	16
10. Messaging/commenting systems (incl. e-mail, learning platforms & more)	19
11. Use of generative AI	20
12. Online storage or learning platforms	21
13. School website	21
14. Digital images and video	21
15. Social media	23
16. Device usage	25
17. National College Courses	27
Appendix 1 – Roles	28
Appendix B: The National Landscape of Online Safety	36
Review Schedule	39

1. Introduction

1.1 Key people / dates

Designated Safeguarding Leads (DSL), with lead responsibility for filtering and monitoring	Chloe Brown (DSL) Craig Smith (DDSL & Online Safeguarding Lead)
Deputy Designated Safeguarding Leads / DSL Team Members	Anita Warren (DDSL) Luke Etheridge (DDSL)

1.2 What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

1.3 Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and is possible to follow in all respects. This will help all stakeholders to understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy will be immediately disseminated to all the above stakeholders.

1.4 Who leads online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

1.5 What were the main online safety risks in 2025/2026?

There are 4 types of online safety risks outlined in KCSIE:

CONTENT: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,

CONTACT: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes,

CONDUCT: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and

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 Online Safeguarding Trends

In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our pupils: children communicating with one another through online games, incidents relating to the use of personal devices outside of school and children not always being kind to one another, 'group chats' where some pupils are not included or pushed out and supervision of personal devices when at home, parents/ carers not always talking to children about what they are using online and who they are talking to and inappropriate use of social media apps and inappropriate access to Youtube.

1.6 How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Part of school induction pack for all new staff (including temporary (sessional), supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school

2. Overview

2.1 Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all school community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.

- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

2.2 Scope

This policy applies to all members of our school community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

3. Roles and responsibilities

Our school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities. Please note there is one for 'All Staff' which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex. All staff have a key role to play in feeding back on potential issues.

4. Education and curriculum

Despite the risks associated with being online, our school recognises the opportunities and benefits to children too. Technology is a fundamental part of adult life and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

It is important that schools establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an

understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils

RSHE guidance also recommends that schools assess teaching and states "The curriculum should build knowledge and skills sequentially, with regular feedback provided on pupil progress. Lessons should ensure that all pupils are challenged, and assessments should identify where pupils need extra support or intervention."

The teaching of online safety features in these particular areas of curriculum delivery:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

However, as stated previously, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what pupils/students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. bias, disinformation, misinformation, and conspiracy theories in line with KCSIE), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

At our school, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why have online safety in our PSHE/Safeguarding curriculum and it is also taught through our computing curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) take place and are used as an opportunity to follow this framework more closely in its key areas. This is done within the context of an annual online safety audit, which is a collaborative effort.

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 our school, 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 need to protect them from harm and prevent future online harm.

We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access.

5. Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Social Media Policy
- Mobile Phone Policy

This school commits to take all reasonable precautions to safeguard pupils online but the internet can never be 100% safe (as stated in KCSIE), and we recognise that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead and Headteacher as soon as possible on the same day. The reporting

member of staff will ensure that a record is made of the concern on CPOMS this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

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.

Any concern/allegation about staff misuse is always (similar to any safeguarding allegation) referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Hub Director and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline 0800 028 0285.

Our school will actively seek support from other agencies as needed. The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online safety incidents involving their children, Children's Services and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

Our school will ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

5.1 Nudes – sharing nudes and semi-nudes

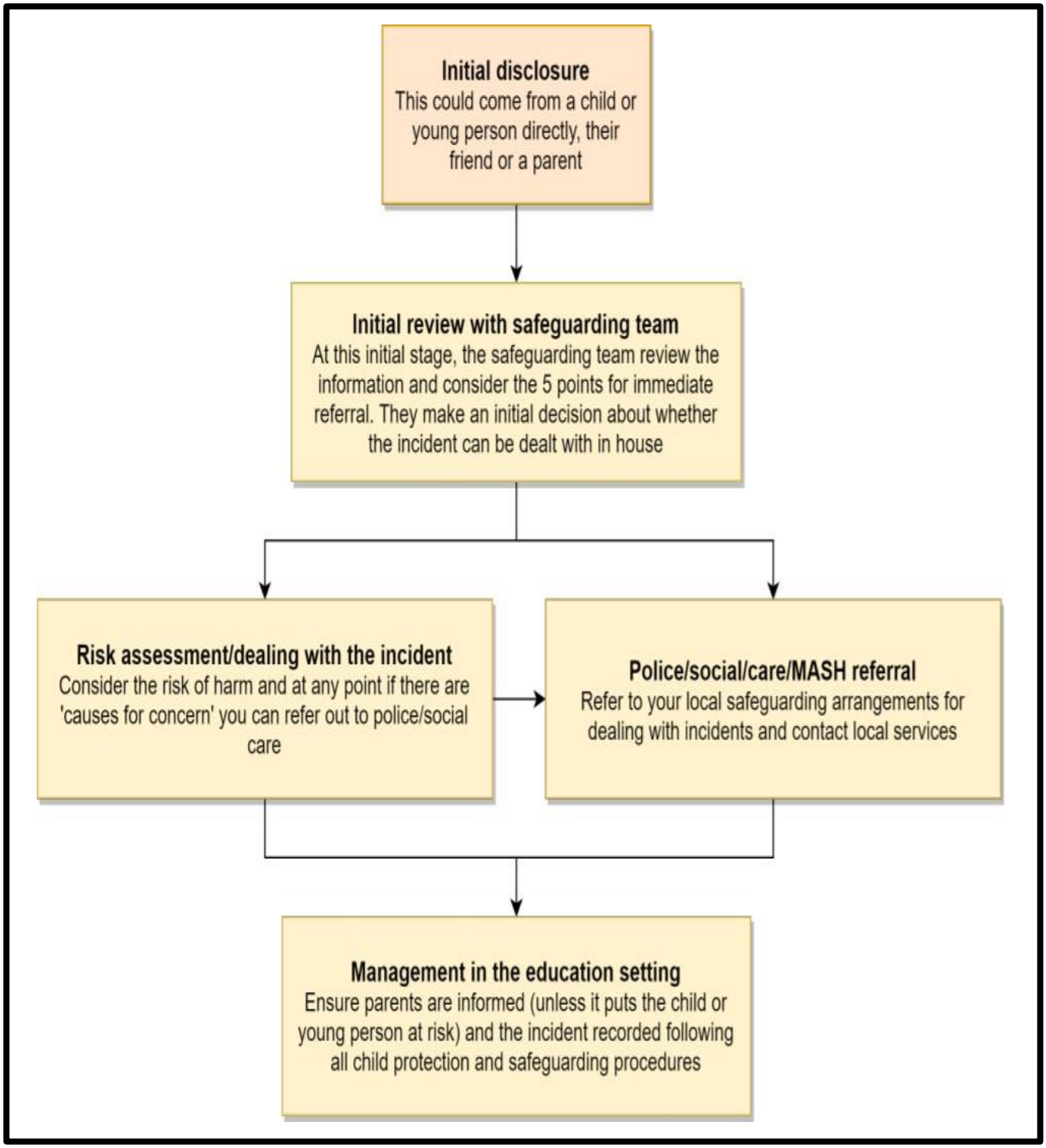
All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - Sharing nudes and semi-nudes: advice for education settings.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.**

It is important that everyone understands that whilst the sharing of intimate or sexual images involving children (created via AI or otherwise) is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or

had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

Our DSL will use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils. The school will also make use of guidance from The Marie Collins Foundation with regards to supporting victims of Technology Assisted Child Sexual Abuse.



5.2 Priority Areas

5.2.1 Upskirting

It is important that everyone understands that upskirting (taking a photo or video of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area. Upskirting has become more prevalent due to the increased use of smart glasses and other discreet recording technology that can capture imagery without individuals knowing.

5.2.2. Bullying

Online bullying (which may also be referred to as cyber bullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed, this includes issues arising from banter.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

5.2.3 Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language. This will be discussed in staff training.

5.3 Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff safeguarding code for adults/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place.

Further to these steps, our school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

5.4 Social media incidents

As of June 2026, the UK Government has announced that social media will be banned for under 16-year-olds. Schools are encouraged to start preparations for this, eg who will manage reports of children accessing social media?]

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy/online safety.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or staff safeguarding code for adults/handbook (for staff). See the social media section later in

this document for rules and expectations of behaviour for children and adults in the school community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), our school will request that the post be deleted and will expect this to be actioned promptly. The police may need to be contacted if an offence is committed. Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

6. CCTV

Our school uses CCTV for the following purposes:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- for the personal safety of pupils, staff, visitors and other members of the public and to act as a deterrent against crime;
- to support law enforcement bodies in the prevention, detection and prosecution of crime;
- to assist in the day-to-day management of the school including ensuring the health and safety of pupils, staff and others;
- for pupil behaviour management (discipline and exclusions); and
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings and associated processes and appeals

We have a CCTV policy which outlines the rationale for use of CCTV, how we balance the use with the right of privacy and how footage is stored, who has access and how long it is stored.

7. Extremism

The school has 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, especially relating to social media, where extremism and hate speech can be easily accessed and highly prevalent on mainstream platforms.

8. Data protection and cyber security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and cyber security policy which can be found here on our website. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Schools should remember that data protection does 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 2025, "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."

9. Appropriate filtering and monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with our Trust Chief Operating Officer and Techminder, our IT support provider, 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.
- 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. Our filtering system is called and it is accredited by the UK Safer Internet Centre.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding, as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out. We ensure all staff are aware of their responsibility in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. Staff can submit concerns at any point to Grace Schools IT Support using the support e-mail address or directly to the DSL and will be asked for feedback at the time of the regular checks, which will now take place.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. They can submit concerns at any point via e-mail and will be asked for feedback at the time of the regular checks which will now take place.

Technical and safeguarding colleagues work together closely to carry out regular reviews and checks and to ensure that the school responds to issues and integrates with the curriculum.

At our school we recognise that generative AI sites can pose data risks so staff are not allowed to enter personal data on any unapproved platform – Google Gemini is our Trust's secure AI platform. Please also refer to our AI Policy. For children and young people, we block the generative AI category via our filtering and only allow specific pre-approved sites. We know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate content can be generated, so we carefully monitor output and limit their use - also in line with DfE guidelines.

Talk Straight is enforced on any accessible search engines on all school-managed devices. Please note however that even with Talk Straight enforced, AI is embedded in many search engine responses and this presents risk to users in terms of misinformation, bias, hallucinations and inappropriate content.

The DSL checks filtering reports and notifications and takes any necessary action as a result.

At school we use Talk Straight for monitoring. According to the DfE standards, "school should have a plan for how to "monitor pupils when using school-managed devices connected to the internet." This could include:

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

Staff Responsibilities include:

- Monitoring what is on a pupil's screen
- Ensuring that unsuitable material is not accessed
- Teaching topics that could create unusual activity on the filtering logs – and advising the IT support accordingly
- Recognising failure in the software or abuse of the system
- Understanding and resolving unreasonable restrictions that affect teaching and learning or administrative tasks
- Noticing abbreviations or misspellings that allow access to restricted material
- Being aware of concerns raised by pupils

10. Messaging/commenting systems (incl. e-mail, learning platforms & more)

10.1 Authorised systems

- Staff at this school use the e-mail system provided by our Trust for all school e-mails. They **never use a personal/private email account** to communicate with children or parents /carers, or to colleagues when relating to school/child data, using a non-school-administered system.
- Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

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 child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an e-mail 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/Headteacher/Data Protection Lead.

10.2 Behaviour / usage principles of messaging/commenting systems

More detail for all the points below are given in the 15. Social section of this policy as well as the school's acceptable use agreements, behaviour policy and staff safeguarding code for adults.

- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Pupils and staff are allowed to use the e-mail system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their e-mails may be read and the same rules of appropriate behaviour apply at all times. E-mails using inappropriate language, images, malware or 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.

11. Use of generative AI

At our school, whilst we acknowledge that generative AI tools such as ChatGPT, Canva, Co-Pilot or Gemini for the creation of new text/imagery/code/music etc, are becoming commonly used by both children and adults, our Trust has strict protocols regarding data protection:

- Google Gemini: This is the Trust's only approved secure AI platform. It is the sole platform authorised for creating school promotional materials (such as posters or flyers) that include pupil photos, provided valid image consent is in place.
- Microsoft Copilot: Authorised for general use, provided no personal data (images, names, or identifying information) is uploaded or shared.
- ChatGPT: Not authorised for use under any circumstances.
- General Rule: No other AI platform is approved for tasks involving personal data.

- We are aware of and follow the DfE's guidance on this and we follow the subsequent principles:

- The use of any Gen AI in our setting (by staff or pupils) will be carefully managed by the school to ensure that users and their data are safe.
- Staff are only permitted to use their school email account when using pre-approved Gen AI, and they must not enter data relating to children, staff or the school which is personal or sensitive (see previous bullets regarding AI tools authorised by our Trust).
- The school has a clear and well communicated approach to the use of any Gen AI (by staff or pupils), and this is aligned with the school's values and pedagogical approaches.
- To help users to safely use technology, we will talk about the use of these tools with pupils, staff and parents – their practical use as well as their safety and ethical pros and cons.
- We are aware that there will be use of these apps and exposure to Gen AI creations on devices at home for many pupils – these experiences may be both positive/creative and also negative (e.g. data breaches, misinformation, bullying, deepfakes, creation of deepfake intimate imagery and chatbots that encourage unhealthy and inappropriate relationships). Therefore, it is important as a school that we support pupils in developing digital literacy skills to help mitigate these risks.

12. Online storage or learning platforms

All the principles outlined above also apply to any IT system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cyber security before adopting such a platform or service and at all times when using it.

13. School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher has delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations. Our Trust provides a website audit document which our school uses to ensure compliance.

The website is managed by school and hosted by an external provider.

Where staff submit 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 – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected.

14. Digital images and video

Our approach to publishing imagery of pupils on our website/social media/marketing materials is to mitigate the risk of data breaches and safeguarding incidents especially in light of concern related to school images being used to create AI generated sexualised imagery of children and staff e.g. we will avoid publishing and sharing any high resolution images of children's faces, but instead only publish lower resolution images of children from behind and in group shots.

When a pupil 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.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database in relation to consent before using it for any purpose.

Any pupils shown in public facing materials are rarely identified with more than first name. Occasionally, a pupil may be holding a certificate of achievement or work they have produced with their name included – it is this possibility that is detailed in our consent forms. 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 school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At our school members of staff may occasionally (i.e. only when school devices are temporarily not available or there are insufficient devices) use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on the school network/cloud platform in line with the retention schedule and the school Data Protection Policy. Any concerns about the nature of these images will be reported to the DSL or Headteacher.

Staff and parents are reminded annually about the importance of not sharing images on social media or otherwise 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. Further detail on this can be found in the Data Protection Policy.

We encourage parents and children to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. 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.

15. Social Media (SM)

15.1 Our SM presence

Our school works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first searching the school online, and the Ofsted pre-inspection check includes monitoring what is being said online.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. We conduct regular checks of privacy and security settings on social media accounts to ensure appropriate access.

15.2 Staff, pupils' and parents' SM presence

As of June 2026, the UK Government has announced that social media will be banned for under 16-year olds. Our school will start preparation for this.

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents / carers have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but schools across our Trust regularly deal with issues arising on social media involving pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. *Note: Children under 13-years can use WhatsApp but only if they have a Parent-Managed Account.*

However, our 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 pupils 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.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Although our school has official social media accounts and will respond to general enquiries about the school, we ask parents/carers not to use these channels, especially not to communicate about their children or to make requests for information (subject access and Freedom of Information Requests).

E-mail is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

Where social media is more widely used as part of school life, e.g. when a Facebook class group is allowed, then at least a second unrelated teacher will be part of the group to monitor activity between the teacher and pupils.

As outlined in the Acceptable Use Policies, pupils are not allowed[1] to be 'friends' with or make a friend request[2] to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might

[1] Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).

[2] Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

not be attributed to the school, trust or local authority, bringing the school into disrepute. Any member of staff who is an online influencer, is not allowed to film content in and about the school.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on 14. Digital images and video and consent is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

16. Device usage

AUPs remind 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. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

16.1 Personal devices including wearable technology and bring your own device (BYOD)

- The DfE has provided statutory guidance to schools and trusts regarding prohibiting the use of mobile phones and smart technology in schools. Please refer to our Mobile Phone and Smart Device Policy for further information regarding this and any exemptions and reasonable adjustments that may apply. The policy applies to pupils, staff, parents, agency workers, governors and trustees, volunteers, visitors and contractors. Where BYOD is allowed, neither staff nor pupils are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.

16.2 Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff safeguarding code for adults.

Wi-Fi is accessible for use of BYOD, guest networks and school-related internet use/ limited personal use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff or pupils are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use. Staff and pupils are not permitted to use Virtual Private Networks (VPNs) on the school network or make any other attempts to bypass the school's filtering. Our filtering is set up to block all use of Virtual Private Networks (VPNs) on school owned devices and across the network.

All and any usage of devices and/or systems and platforms may be tracked.

16.3 Trips / events away from school

For school trips/events away from school, teaching staff will be issued with a school duty phone and this number will be used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teaching staff using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or pupil accessing a member of staff's private phone number.

If on trips pupils are encouraged to connect to another organisation's Wi-Fi/network, staff must be aware that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in school and therefore staff are responsible for risk assessing and managing such situations. Staff should seek advice from the DSL where necessary.

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.

Our school will ensure that the authorised systems we use to communicate with parents as outlined within policy include any systems used in exceptional circumstances, such as on trips, for example notifying parents of trip updates or status of arriving back at school, and that these notifications are data protection compliant.

16.4 Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Headteacher and staff authorised by them have a statutory power to search pupils' property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy and in the Trust Mobile Phone and Smart Device Policy