



Hazelwood Schools

Online Safety Policy

Reviewed and Adopted: **Autumn 2025**

Reviewed by: FGB

Next Review: **Autumn 2027**

Review every two years

Adapted from LGFL Online Safety Policy found at safepolicies.lgfl.net

LGfL

DigiSafe
Keeping children safe

Introduction

Key people / dates

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Samantha Powell
Deputy Designated Safeguarding Leads / DSL Team Members	Josh Newham, Erina Komodromos, Crissy Walls, Sarah Hatswell
Link governor for safeguarding	Sarah Naughton and Ash Venn

Overview

Aims

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

- Setting out expectations for all Hazelwood Schools 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.
- 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 and 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).

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with our Safeguarding Children and Child Protection Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO).

Beyond this, [reporting.jgfl.net](https://www.reportit.org.uk/) has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

Scope

This policy applies to all members of the Hazelwood Schools 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.

Roles and Responsibilities

This 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; 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.

It is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

All Staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the schools' main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the DSL and ensure that the responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- 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
- 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
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors 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 suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead and Safeguarding Team

Key responsibilities (*remember 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
- 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 pupils 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 1
 - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- 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 with the headteacher, DPO and governors 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 Prevent awareness training”
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based and submit for review to the governors
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends

- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance and beyond, in wider school life
- 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 adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site
- 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).

Governing Body

Key responsibilities *(quotes are taken from Keeping Children Safe in Education)*

- Approve this policy and strategy and subsequently review its effectiveness
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher 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
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety) and now also reminders about filtering and monitoring
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum

PSHE / RSHE Leads

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. “This will include being taught what positive, healthy

and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."

- Focus on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#) in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Work closely with the Computing subject leads to identify cross curricular links and ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Leads

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the PSHE/RSHE leads to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Data Protection Officer (DPO)

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training, and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- 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 2023, "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."
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- The information for the DPO can be found on the school website.

Volunteers and Contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)

- Report any concerns, no matter how small, to the DSL
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications

Parents/Carers

Key responsibilities:

- Read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and 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, pupils or other parents/carers.

External Groups including Parent Associations

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, pupils or other parents/carers

Education and Curriculum

Despite the risks associated with being online, Hazelwood Schools 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.

The following subjects have the clearest online safety links

- PSHE including RSHE
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

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. disinformation, misinformation, and conspiracy theories in line with KCSIE 2025), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

Annual reviews of curriculum plans (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

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.

Handling Online-Safety Concerns and Incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE and RSHE).

General 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 err on the side of talking to the DSL to contribute to the overall picture or highlight what might not yet be a problem. If in doubt always log concerns.

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 (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding Children and Child Protection Policy
- Child-on-Child Abuse Policy
- Behaviour and Anti-Bullying Policy
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation
- Complaints Policy
- Staff Code of Conduct
- PSHE Policy
- RSHE Policy

This school commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises 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 online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. This can be done in person or via Safeguard. This includes any concerns raised by the filtering and monitoring systems.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed.

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting).

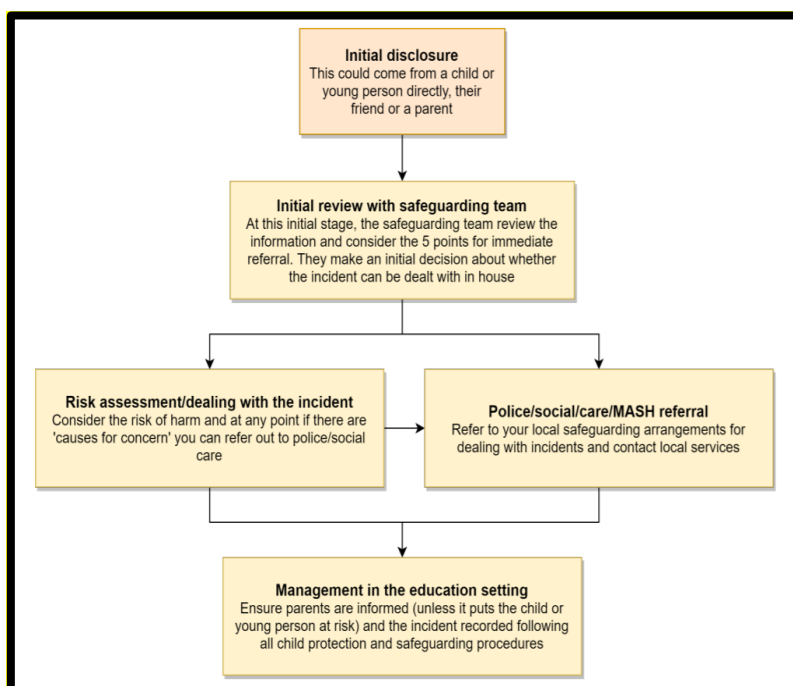
The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Nudes – sharing nudes and semi-nudes

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 nudes involving children 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 school 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.



Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now 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.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

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 full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

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.

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 code of conduct/handbook.

Further to these steps, the 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.

Social Media Incidents

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 code of conduct/handbook (for staff). See the social media section later in this document for rules and expectations of behaviour for children and adults in the Hazelwood Schools 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, Hazelwood Schools will request that the post be deleted and will expect this to be actioned promptly.

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.

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 widespread on certain platforms.

Data Protection and Cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children.

Appropriate Filtering and Monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with staff 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 look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

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

At our school we recognise that generative AI sites can pose data risks so staff are not allowed to enter child data and where they use them, they must be approved. For children and young people, we block the generative AI category and only allow specific 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.

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.

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

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools. In addition:

- web filtering is provided by LGfL on school site and for school devices used in the home
- changes can be made by EN Digital and the School Business Manager, Catherine Findlater
- overall responsibility is held by the DSL

- technical support and advice, setup and configuration are from ENDigital
- regular checks are made half termly by ENDigital and the School Business Manager to ensure filtering is still active and functioning everywhere. These are evidenced on the school Google Drive
- an annual review is carried out as part of the online safety audit to ensure a whole school approach

At home, school devices are monitored by LGfL filtering when on home wifi connections.

When pupils log into their Google Workspace account on a personal device, activity may also be monitored there.

Digital Images and Video

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. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media
- For a specific high-profile image for display or publication

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

Any pupils shown in public facing materials are never identified with more than 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 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 Hazelwood, no member of staff should ever use their personal phone to capture photos or videos of pupils. However, members of staff may occasionally use personal phones when a school device is not available, 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.

Photos are stored on the Google Drive in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded regularly about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

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.

Use of Generative AI

At Hazelwood Schools, we acknowledge that generative AI platforms (e.g. ChatGPT or Gemini for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the [DfE's guidance](#) on this. In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons where appropriate.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, nudifying apps and inappropriate chatbots).
- Staff are trained in the use of AI and the impact it can have both positively and negatively.
- AI tools are used as part of the computing curriculum and staff are supported to use AI to assist in planning and report writing, where personal data is not used.

Behaviour / Usage Principles

- 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.
- Staff are allowed to use the email system for reasonable (not excessive, not during lessons) 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 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).

Social Media

The Schools' Social Media Presence

Hazelwood Schools 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 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

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.

The headteacher is responsible for managing our Social Media presence and checking our Google reviews. They follow the guidance in the LGfL / Safer Internet Centre online-reputation management document.

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 day-to-day responsibility.

The site is managed by / hosted by E4 Education.

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.

Staff, Pupils' and Parents' Social Media Presence

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 have a concern about the school, we would 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 the school regularly deals with issues arising on social media involving pupils/students 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.

However, 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 pupils/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.

Email is the official electronic communication channel between parents and the school.

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 not be attributed to the school, trust or local authority, bringing the school into disrepute.

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 Digital Images and Video and permission 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 (see nofilming.lgfl.net for more information). 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.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

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.

Use of Mobile Phones

- **Hazelwood Schools is a Smartphone Free School**
- **Pupils in Year 6** are allowed to bring “brick” mobile phones in for their journey to and from school. During the school day, phones must be handed in to the class teacher and remain turned off at all times. Any attempt to use a phone during the school day without permission will lead to an internal exclusion. Likewise, if a child is found with a smartphone, this will result in the phone being confiscated by the headteacher. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the ‘Digital images and video’ section of this document and the school data protection policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they should notify a member of Senior Leadership Team.
- **Volunteers, contractors, governors** should leave their phones turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones turned off 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. When at school events, please refer to the Digital images and video section of this document.

Use of Smartwatches

- Smartwatches are not allowed to be worn in school by any pupil due to the potential risks associated such as: making and receiving phone calls and messages; recording of video and audio; access to social media.

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 code of conduct.

Wifi is accessible to all stakeholders and agreed visitors for 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 students 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.

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

Trips / Events Away from School

For school trips/events away from school, staff using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

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.

Monitoring

As part of our monitoring strategy we will:

- Regularly review this policy in line with KCSIE and current issues within the school and local/national context
- Share with Governors any relevant information and data around online safety
- Include this policy as part of our induction pack for all staff and volunteers