

Winchester House School

Online Safety and Digital Awareness Policy

Version 1

Responsible Governor:

Adopted by Governors:

Last Reviewed: 1st September 2026 (SJP)

Next review due: 1st September 2027 (Deputy Head Pastoral)

Introduction

Aims and Context

Digital technologies are an integral part of teaching, learning and everyday life for children, young people and adults. This policy, together with the School's Acceptable Use Policies, aims to support all members of the Winchester House community in using technology safely, responsibly, respectfully and confidently.

The School recognises that technology offers significant educational and social benefits. However, it also presents potential risks, including exposure to inappropriate content, cyberbullying, technology-facilitated abuse, harmful online interactions, misinformation, online exploitation and the misuse of artificial intelligence (AI) and emerging technologies.

By maintaining a secure and well-managed technical infrastructure, providing effective online safety education and establishing clear expectations for behaviour both online and offline, Winchester House seeks to protect the safety, wellbeing and reputation of all members of the school community.

Digital technologies include, but are not limited to, internet-enabled devices, online platforms, cloud-based services, social media, messaging services, gaming platforms, artificial intelligence tools, wearable technology and digital communication systems. Recognising the rapid pace of technological change, this policy sets out principles and expectations that apply regardless of the specific device, platform or technology being used.

Online safety is an essential part of safeguarding. Concerns relating to online behaviour, cyberbullying, technology-facilitated abuse, harmful sexual behaviour, child-on-child abuse or other safeguarding matters will be managed in accordance with the School's Safeguarding and Child Protection Policy and recorded through the School's safeguarding procedures.

As with all safeguarding matters, it is important that concerns are identified, reported and addressed promptly. This policy outlines how members of the school community can seek support, report concerns and respond appropriately when online safety issues arise.

Scope of this Policy

This policy applies to all members of the Winchester House community, including:

- Governors
- Staff
- Pupils
- Volunteers
- Parents and carers
- Visitors
- Contractors and third-party providers working on behalf of the School

This policy applies to the use of digital technologies, online services and electronic communications both within and beyond the School environment. It applies whenever an individual's online activity has an impact on the safety, wellbeing or reputation of members of the Winchester House community, regardless of the device, platform or location involved.

The School recognises that online behaviour can have real-world consequences. Online conduct is therefore subject to the same expectations of kindness, respect and responsibility that apply offline and should reflect the values of The Winchester House Way.

Under the Education and Inspections Act 2006, the Head has the authority to regulate pupil behaviour outside school where it is reasonable to do so. This may include incidents involving cyberbullying, technology-facilitated abuse, online misconduct, inappropriate use of digital technology or other online safety concerns that occur away from the School site but are linked to a pupil's membership of the School or have an impact on the safety, wellbeing or orderly running of the school community.

Safeguarding

Online safety is a core element of safeguarding at Winchester House. The School recognises that safeguarding concerns can arise both offline and online and that the same child-centred approach applies in all circumstances.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content (including content generated using artificial intelligence), for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), conspiracy theories, and deepfake content;
- **contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this (for example, AI chatbots); 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 artificial intelligence), online bullying, technology-facilitated abuse, and the consensual and non-consensual sharing of nudes and semi-nudes; and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing, financial scams, AI-enabled fraud, and data theft.

The School recognises that online safeguarding concerns may include child-on-child abuse, cyberbullying, harmful sexual behaviour, technology-facilitated abuse, image-based abuse, sextortion, online harassment, the misuse of artificial intelligence (AI), and the creation or sharing of manipulated or deceptive digital content.

The School also recognises that children and young people may be vulnerable to online grooming, child sexual exploitation, criminal exploitation, radicalisation and extremism. These risks are addressed through the School's safeguarding arrangements and Prevent Duty responsibilities.

To help safeguard pupils online, Winchester House:

- Maintains appropriate filtering and monitoring systems across school networks and devices.
- Ensures the Designated Safeguarding Lead (DSL), who has lead responsibility for online safety, works closely with the Group Director of ICT to oversee filtering, monitoring and online safeguarding arrangements.
- Embeds online safety education throughout the curriculum, in line with the Department for Education's *Teaching Online Safety in Schools* guidance.
- Provides regular safeguarding and online safety training for staff.
- Promotes digital resilience, critical thinking and responsible technology use.
- Encourages pupils to report concerns, seek support and act safely and responsibly online.

Concerns relating to online safety, cyberbullying, technology-facilitated abuse, child-on-child abuse or any other safeguarding matter will be managed in accordance with the School's Safeguarding and Child Protection Policy and recorded through the School's safeguarding procedures.

Roles and Responsibilities

This section outlines the roles and responsibilities for **online safety** across the Winchester House community.

Governors

- Governors are responsible for approving the Online Safety and Digital Awareness Policy and reviewing its effectiveness annually.
- The Safeguarding Governor is informed of any significant online safety incidents by the Head and/or Designated Safeguarding Lead (DSL).
- Governors receive appropriate updates and assurance regarding the School's filtering, monitoring and online safeguarding arrangements.
- The Designated Safeguarding Lead (DSL) maintains secure safeguarding records, including incidents involving digital technologies. Relevant themes, trends and actions are reported to Governors through the DSL's safeguarding reporting processes.

The Head and Senior Leaders

- The Head has overall responsibility for ensuring the safety and wellbeing of all members of the school community, including online safety.
- The Designated Safeguarding Lead (DSL) has lead responsibility for online safety and works closely with the Group Director of ICT to oversee filtering, monitoring and online safeguarding arrangements.
- The Head ensures that DSLs and other relevant staff receive appropriate training and continuing professional development (CPD) to fulfil their online safety responsibilities.
- Senior leaders will ensure that online safety is embedded within the School's wider safeguarding culture, curriculum and pastoral systems.
- In the event of an allegation against a member of staff involving online conduct or digital technologies, the procedures outlined within the Safeguarding and Child Protection Policy will be followed. Referral to the Local Authority Designated Officer (LADO) will be considered where appropriate.

Designated Safeguarding Leads (DSLs)

- Simon Preece (Designated Safeguarding Lead)
- Vicki Berrie (Deputy DSL)
- Kate Badenoch (Deputy DSL)
- Emma Gillies (Deputy DSL)
- Tom Gray (Deputy DSL)
- Amy Shaw (Deputy DSL)

DSLs should maintain an up-to-date understanding of online safety and emerging technologies and be aware of safeguarding concerns arising from:

- The sharing of personal information and data online.
- Access to illegal, harmful or inappropriate content.
- Online gambling, scams, fraud and financial exploitation.
- Making, sending or receiving nude or semi-nude images, including AI-generated content.
- Child-on-child abuse.
- Harmful sexual behaviour.
- Inappropriate online contact with adults or strangers.

- Grooming, exploitation and coercion.
- Cyberbullying, prejudice-based bullying and discriminatory bullying.
- Technology-facilitated abuse.
- Artificial intelligence, deepfakes and manipulated digital content.
- Radicalisation and extremism.

The DSLs will:

- Lead the development, implementation and annual review of the Online Safety and Digital Awareness Policy.
- Take lead responsibility for online safety safeguarding matters.
- Work closely with the Group Director of ICT regarding filtering, monitoring and technical safeguarding arrangements.
- Receive, record and respond to reports of online safety concerns.
- Ensure online safety concerns are managed in accordance with the School's safeguarding procedures.
- Ensure staff, including Governors, receive appropriate online safety training.
- Ensure pupils receive age-appropriate online safety education.
- Support parents and carers through the provision of online safety information and guidance.
- Report relevant online safety matters to the Senior Leadership Team and Governors as appropriate.

Teaching and Support Staff

All staff are responsible for:

- Maintaining an up-to-date understanding of the School's Online Safety and Digital Awareness Policy.
- Reading, understanding and adhering to the Staff Acceptable Use Policy, Staff Code of Conduct and relevant safeguarding procedures.
- Modelling safe, responsible and professional use of technology.
- Promoting and reinforcing the expectations set out in the Pupil Acceptable Use Policy.
- Embedding online safety messages within teaching and everyday interactions with pupils where appropriate.
- Reporting any online safety concern, safeguarding concern or suspected misuse of technology in accordance with the School's safeguarding procedures.

Pupils

Pupils are expected to:

- Read, understand and follow the Pupil Acceptable Use Policy.
- Use digital technologies safely, responsibly and respectfully, reflecting the values of The Winchester House Way.
- Report any online safety concern, cyberbullying, misuse of technology or worrying online behaviour to a trusted member of staff.
- Seek help if they encounter content, contact or conduct that makes them feel unsafe or uncomfortable.

Parents and Carers

Parents and carers play a vital role in helping children use technology safely and responsibly. They are encouraged to:

- Support and reinforce the expectations set out in the Pupil Acceptable Use Policy.
- Follow the guidance contained within this policy and other relevant school procedures.
- Work in partnership with the School to promote safe and positive online behaviour.
- Engage with information, communications and resources provided by the School regarding online safety.

- Raise concerns promptly with the School where online safety issues may affect a pupil's wellbeing, safety or education.

Infrastructure and Access Control

- Servers, wireless systems and network infrastructure are securely managed, with appropriate physical and technical security measures in place.
- Access to the School's IT systems is granted according to role and responsibility, with users only being given access to the systems and information necessary for their work or learning.
- Each user is provided with a unique username and password. In Bradshaw and Seligman, group logins may be used under staff supervision where appropriate.
- Users must keep their passwords secure and must not share login credentials with others unless authorised arrangements are in place.
- Staff and pupils must report any suspected compromise of login credentials, unauthorised access or security breach immediately.
- Appropriate authentication measures, including password controls and, where applicable, multifactor authentication, will be used to help protect school systems and data.
- User accounts, permissions and access rights will be reviewed periodically to ensure that access remains appropriate and secure.

Filtering and Monitoring

Winchester House uses appropriate filtering and monitoring systems to help safeguard pupils and staff when using school networks, devices and online services. These systems are designed to reduce the risk of access to illegal, inappropriate or potentially harmful content and to identify behaviour that may indicate a safeguarding concern.

Filtering systems are designed to prevent access to content that is considered harmful or unsuitable, including, but not limited to, material that:

- Promotes or glorifies violence.
- Promotes criminal, illegal or harmful activity.
- Contains racist, discriminatory or hateful content.
- Promotes extremism, radicalisation or terrorism.
- Contains pornographic, sexually explicit or otherwise age-inappropriate material.
- Includes offensive, abusive or profane language.
- Encourages self-harm, suicide or other harmful behaviours.
- Is misleading, deceptive or generated to cause harm, including certain forms of AI-generated content.
- Breaches legislation relating to copyright, data protection or computer misuse.

Monitoring systems are used to help identify potential safeguarding concerns, inappropriate use of technology and other activity that may place members of the school community at risk. Monitoring is conducted in accordance with safeguarding, data protection and other relevant legal requirements.

Requests to unblock websites or online services for educational purposes will be reviewed by the Group Director of ICT and, where appropriate, the DSL.

Filtering and monitoring arrangements are reviewed regularly to ensure that they remain effective, proportionate and appropriate to the needs of the School.

The School recognises that filtering systems cannot eliminate all risks and that no technical solution can provide complete protection. Filtering and monitoring therefore form part of a wider safeguarding approach that includes education, supervision, staff training and clear reporting procedures.

Where personal devices access the internet using mobile data (3G, 4G or 5G), the School's filtering systems may not apply. Guidance regarding the safe use of personal devices is provided within the relevant Acceptable Use Policies (AUPs).

Reporting and Security

All members of the Winchester House community share responsibility for maintaining a safe and secure digital environment.

- Any actual or suspected online safety concern, safeguarding concern, misuse of technology or security incident must be reported promptly through the School's safeguarding and reporting procedures, including MyConcern in accordance with the School's safeguarding procedures.
- Users must report any suspected unauthorised access, security breach, compromised account, loss of school data or other incident that may affect the security of the School's systems or the safety of members of the school community.
- Appropriate technical and organisational security measures are in place to protect the School's networks, servers, devices, systems and data from accidental, inappropriate or malicious access, damage, loss or disruption.
- Online safety incidents will be managed in accordance with the School's Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy and Staff Code of Conduct, as appropriate.

The Staff and Pupil Acceptable Use Policies (AUPs) provide detailed guidance regarding the use of school technology and systems and include expectations relating to:

- The downloading or installation of software.
- The use of removable media and external storage devices.
- Access to school networks, systems and online services.
- The handling, storage and sharing of personal, confidential or sensitive information.
- Appropriate and responsible use of digital technologies both within and beyond the School environment.

Online Safety Education – Pupils

Children and young people require the support of Winchester House to recognise, understand and manage online risks whilst developing the knowledge, skills and confidence to use technology safely, responsibly and positively.

As part of this commitment, Winchester House operates as a smartphone-free site. Pupils are not permitted to bring smartphones or similar personal devices into school. This supports learning, wellbeing, positive social interaction and the development of healthy relationships with technology.

The aim of the School's online safety education is to empower pupils to make informed, responsible and respectful choices when using digital technologies. Pupils should develop the knowledge and skills needed to protect their safety, wellbeing, reputation and personal information whilst benefiting from the educational and social opportunities that technology provides.

Delivery of Online Safety Education

Online safety education will be delivered in age-appropriate ways across the school, including through:

- Computing and digital literacy lessons.
- Planned teaching within the PSHE curriculum.
- Tutor time activities.
- Assemblies and whole-school messages.
- Wider curriculum opportunities where online safety issues arise naturally.

Where age-appropriate AI tools are used to support teaching and learning, their use will be appropriately

supervised and risk-assessed, with account taken of safeguarding, privacy and data protection considerations.

Curriculum Focus

Online safety education will reinforce pupils' understanding of the main areas of online risk identified within the 4Cs framework: Content, Contact, Conduct and Commerce.

Teaching will help pupils to:

- Recognise harmful, misleading or inappropriate online content, including misinformation, disinformation and deepfake content.
- Understand safe online interactions and how to respond to unwanted contact, grooming, manipulation or exploitation.
- Recognise cyberbullying, technology-facilitated abuse and harmful online behaviour.
- Understand the risks associated with making, sharing or receiving nude or semi-nude images.
- Develop critical thinking skills and evaluate the reliability and accuracy of online information.
- Understand how artificial intelligence (AI) and emerging technologies can be used positively whilst recognising associated risks and limitations.
- Understand digital footprints, online reputation and the long-term impact of online behaviour.
- Identify and avoid online scams, phishing attempts, financial risks and deceptive online practices.
- Develop healthy habits relating to screen use, online relationships and personal wellbeing.

Embedding Online Safety Across the Curriculum

Online safety should be promoted across all areas of school life. Staff are expected to reinforce safe practices, responsible behaviour and critical thinking whenever appropriate opportunities arise.

For example:

- Pupils should understand and follow the Pupil Acceptable Use Policy (AUP).
- Pupils should be encouraged to use technology safely, responsibly and respectfully, both in and out of school, reflecting the values of The Winchester House Way.
- Pupils should be taught to evaluate online content critically and verify the accuracy of information obtained from digital sources.
- Pupils should learn to acknowledge sources appropriately and respect copyright and intellectual property when using online materials.
- Pupils should understand that online behaviour can have real-world consequences and that the same expectations apply online as offline.

Safe Use of Technology in Lessons

When planning lessons that involve internet use:

- Staff should guide pupils towards pre-checked, age-appropriate websites and resources wherever possible.
- Where pupils are permitted to search independently, staff should provide appropriate supervision and monitoring.
- Where sensitive topics require access to sites or content that may otherwise be restricted, requests for access should be made through the School's established procedures and be clearly justified and auditable.

Online Safety Training – Staff

All staff must receive appropriate online safety training to enable them to safeguard pupils effectively and promote the safe and responsible use of technology.

For most teaching and support staff, as well as Governors, this will be achieved through:

- Safeguarding induction.
- Regular safeguarding and online safety updates.
- Annual safeguarding training delivered by the Designated Safeguarding Leads (DSLs).

Training will ensure that staff understand:

- The online risks that children and young people may encounter.
- Their responsibilities under this policy and related safeguarding procedures.
- The risks associated with personal and professional use of technology.
- The appropriate action to take in response to online safety, safeguarding or security concerns.
- Emerging technologies and online risks, including artificial intelligence (AI), deepfakes and technology-facilitated abuse.

Designated Safeguarding Leads (DSLs)

DSLs will maintain an appropriate level of expertise in online safety and will:

- Be equipped to respond effectively to online safety safeguarding concerns.
- Understand and interpret monitoring and safeguarding reports relating to the School's digital systems.
- Advise on the development and delivery of online safety education.
- Support and train colleagues.
- Provide guidance and resources for parents and carers.
- Maintain awareness of emerging technologies, trends and safeguarding risks.

Online Safety Guidance – Parents and Carers

Winchester House recognises the vital role that parents and carers play in supporting children to use technology safely, responsibly and respectfully.

The School will seek to provide parents and carers with relevant and up-to-date information to help them understand online risks, promote positive online behaviour and support their children's wellbeing in a digital world.

Information may be shared through:

- The School website.
- Parent communications and bulletins.
- Information sessions, workshops or presentations where appropriate.
- Online safety resources and guidance published by the School.

Parents and carers are encouraged to work in partnership with the School and to raise concerns promptly where online activity may affect a pupil's safety, wellbeing or education.

Definition of Personal Devices

For the purposes of this policy, a personal device is any portable equipment capable of connecting to the internet, storing or transmitting data, capturing images, recording audio or video, or supporting digital communications.

This includes, but is not limited to:

- Mobile phones
- Laptops
- Tablets
- Smart watches, smart glasses and other wearable technology
- Cameras
- Audio or video recording devices
- Any other internet-enabled, data-enabled or image-capturing device

Staff Responsibilities

When working with pupils, staff must always prioritise the safety, wellbeing and best interests of the children in their care.

All staff are expected to:

- Use technology safely, responsibly and professionally.
- Adhere to the Staff Acceptable Use Policy, Staff Code of Conduct and Data Protection Policy.
- Model positive digital behaviour at all times.
- Maintain appropriate professional boundaries when using digital technologies and online communication.
- Report any safeguarding concern, security concern or misuse of technology in accordance with the School's safeguarding procedures.

Failure to comply with this policy or associated policies may result in disciplinary action being taken in accordance with school procedures.

Device Use

Winchester House recognises that staff may need to use personal devices for legitimate professional purposes. Such use must always be consistent with safeguarding, data protection and professional conduct expectations.

Examples of appropriate professional use may include:

- Accessing school communication systems.
- Taking registers.
- Communicating with colleagues.
- Supporting the supervision of pupils during activities, trips or educational visits.
- Accessing school email systems through appropriately secured devices.

All use of personal devices for school-related purposes must comply with the Staff Acceptable Use Policy, Staff Code of Conduct and Data Protection Policy.

Additional expectations regarding mobile phones, wearable technology, photography, video recording and the use of personal devices in Early Years settings are set out within the Staff Code of Conduct and relevant Acceptable Use Policies.

Offsite Visits and Educational Visits

When using digital technology during educational visits, fixtures, residential trips or other activities away from the School site, staff must continue to follow the expectations set out in this policy, the Staff Code of Conduct, the Staff Acceptable Use Policy and the School's safeguarding procedures.

- School-provided devices should be used for communication with pupils and parents/carers wherever reasonably practicable.
- Any personal data stored on devices for the purposes of a visit must be handled securely and deleted when no longer required.
- Where a pupil requires access to a mobile device during an educational visit, a school-provided device should be used where possible.
- In exceptional circumstances, and where no suitable school device is available, a member of staff may permit supervised use of their own device, ensuring appropriate safeguarding, privacy and professional boundaries are maintained.
- Staff should ensure that the use of digital technology during visits supports the safety, welfare and effective supervision of pupils at all times.

Use of Digital Photographic and Video Imagery

Staff must only use school-approved equipment and systems when capturing, storing, sharing or publishing photographic or video imagery of pupils.

All imagery must:

- Be transferred only to school-approved systems.
- Be stored securely in accordance with the School's safeguarding and data protection procedures.
- Be shared only through authorised school communication channels or agreed internal processes.

The use of personal devices for capturing photographic or video imagery of pupils is prohibited except in the exceptional circumstances outlined within the Staff Code of Conduct.

Consent and Context

When capturing or using images of pupils:

- Pupils should be made aware when imagery is being taken wherever practicable.
- Staff must ensure that pupils are appropriately dressed and not participating in activities that could place them at risk of embarrassment, exploitation or unwanted attention.
- Images should be selected and used in a manner that protects the dignity, wellbeing and privacy of pupils.
- Images published through school channels will comply with relevant safeguarding, data protection and consent requirements.

Artificial Intelligence and Image Manipulation

The School recognises that advances in artificial intelligence (AI) and other digital technologies have increased the risks associated with digital imagery and media. Images, audio and video content may be copied, manipulated, altered or shared beyond their original intended purpose.

Any use of AI-generated, enhanced or manipulated imagery involving pupils must be lawful, appropriate, ethical and consistent with the School's safeguarding, data protection and publication procedures. When capturing, storing and publishing imagery, the School will take reasonable steps to safeguard pupils' privacy, wellbeing and digital identity whilst continuing to celebrate and promote school life appropriately.

The creation, possession or sharing of misleading, harmful or inappropriate manipulated content involving pupils may be treated as a safeguarding concern and managed in accordance with the School's safeguarding procedures.

Parental Permissions

The School will respect the image-use preferences and permissions provided by parents and carers.

Where permission has not been given for a pupil's image to be published, staff must ensure that such imagery is not used in publications, marketing materials, websites, social media platforms or other public-facing communications.

Privacy and Identification

To help safeguard pupils' privacy:

- Pupils' full names, home addresses or other personal information will not normally be published alongside imagery on public-facing platforms.
- Care will be taken to ensure that published content does not unintentionally reveal sensitive personal information about pupils or their families.

Exceptional Circumstances – Use of Personal Devices for Imagery

The School's expectation is that photographic and video imagery of pupils will be captured only using school-approved equipment and systems.

In exceptional circumstances, where no suitable school equipment is available and the educational or operational need is clear, the Head or Deputy Head (Pastoral) may authorise the temporary use of a personal device.

Where such authorisation is granted:

- The use must be appropriate, necessary and consistent with safeguarding requirements.
- The device must be secured appropriately.
- Images must be transferred to a school-approved system as soon as reasonably practicable.
- Images must be deleted from the personal device immediately following transfer.
- Images must only be used for approved school purposes and in accordance with the School's safeguarding, data protection and publication procedures.

Any such use must be exceptional, pre-approved where practicable, and capable of being justified and audited.

Commissioned Photographers and External Providers

Commissioned photographers and other external providers must comply with the School's safeguarding, data protection and publication requirements.

The member of staff responsible for commissioning the provider must ensure that:

- Images are captured only for the agreed purpose.
- Pupils are aware that imagery is being taken.
- Pupils are appropriately dressed and participating in suitable activities.
- Images are stored and transferred securely.
- Images are not shared or used beyond the agreed purpose.
- Any use of imagery complies with parental permissions and the School's safeguarding requirements.

Written agreements or contractual arrangements should clearly set out ownership, storage, use and retention arrangements for any imagery produced on behalf of the School.

Visitors, Volunteers and Current/Prospective Parents

Winchester House recognises that visitors, volunteers and parents may bring personal devices onto the school site. However, safeguarding, privacy and the wellbeing of pupils remain paramount.

Visitors are expected to:

- Use personal devices responsibly and in accordance with the School's safeguarding expectations.
- Avoid the use of personal devices when working directly with or supervising pupils unless authorised by the supervising member of staff.
- Hand in personal devices on arrival when visiting areas of the School where this is required, including Bradshaw.
- Refrain from taking photographs, video recordings or audio recordings of pupils unless specifically authorised or commissioned by the School.
- Follow any additional safeguarding guidance provided during their visit.

Visitors requiring access to the School's WiFi network must:

- Use only the access credentials provided by the School.
- Comply with the School's Acceptable Use Policy and any conditions of network access.

Parents, carers and visitors who take photographs or videos at school events are expected to do so for personal use only and must do so in a manner that respects the privacy and safeguarding of all members

of the school community. The publication or sharing of images should take account of the privacy of other children and families and comply with any guidance issued by the School.

These arrangements are intended to safeguard pupils, protect privacy and support the secure use of technology across the School community.

Online Communication

For the purposes of this policy, online communication refers to any digital platform that enables users to communicate, collaborate, create, publish or share content. This includes, but is not limited to, email, messaging services, social media platforms, online forums, blogs, gaming platforms, livestreaming services and other digital communication tools.

Winchester House recognises that online communication can support learning, creativity, collaboration and positive engagement within the school community. However, online activity should reflect the same standards of behaviour, respect and responsibility that are expected offline and should be consistent with the values of The Winchester House Way.

All members of the school community should be aware that content shared online may be copied, stored, altered or distributed beyond its original audience and may remain accessible indefinitely. Individuals should therefore consider carefully the impact of any content they create, share or respond to online.

Online communication should not be used to:

- Bully, harass, intimidate or discriminate against others.
- Engage in cyberbullying, technology-facilitated abuse or other behaviour that may place others at risk.
- Share, create or distribute harmful, misleading or inappropriate content.
- Share confidential, personal or sensitive information without appropriate authority.
- Damage the reputation, safety or wellbeing of individuals or the wider school community.

The School expects all members of the community to communicate online in a respectful, responsible and lawful manner. Online behaviour that raises safeguarding concerns or breaches school expectations may be addressed in accordance with the School's Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct and Acceptable Use Policies, as appropriate.

Remote Learning and Live Online Communication

Where remote learning or live online communication is required, the School will take reasonable steps to ensure that interactions take place safely and appropriately through approved platforms and systems.

Pupils and parents should be aware that:

- Pupils should be appropriately dressed for live online sessions.
- Pupils should participate from a suitable shared area within the home wherever reasonably possible and not from private spaces without appropriate supervision.
- Parents and carers should provide age-appropriate oversight and support.
- Live online communication should take place through school-approved platforms and in accordance with the School's safeguarding procedures.

Responding to Online Safety Concerns, Misuse and Inappropriate Content

Winchester House expects all members of the school community to use digital technologies safely, responsibly and in accordance with this policy. Where concerns arise, they will be addressed promptly, proportionately and in line with the School's safeguarding procedures.

Safeguarding Concerns

Any online activity that raises a safeguarding concern must be reported immediately in accordance with the School's safeguarding procedures and recorded through the appropriate reporting systems, including MyConcern where appropriate.

Examples of concerns may include:

- Child-on-child abuse.
- Cyberbullying or technology-facilitated abuse.
- Harmful sexual behaviour.
- Grooming, exploitation or coercion.
- Sextortion.
- The creation, possession or sharing of nude or semi-nude images.
- Exposure to harmful, extremist or illegal content.
- The misuse of artificial intelligence (AI) or manipulated digital content in a manner that causes harm.
- Any other online behaviour that may place a child at risk of harm.

Serious safeguarding concerns must be referred to the Designated Safeguarding Lead (DSL) without delay and managed in accordance with the School's Safeguarding and Child Protection Policy.

Where appropriate, concerns may also be referred to external agencies, including the police, children's social care or the National Crime Agency's CEOP Safety Centre.

Misuse of Technology

Incidents involving inappropriate use of technology that do not meet safeguarding or criminal thresholds should still be reported promptly so that they can be investigated and addressed appropriately.

Examples may include:

- Breaches of the Acceptable Use Policies.
- Unauthorised access to systems or accounts.
- Inappropriate use of school devices or networks.
- Breaches of data protection or information security procedures.
- Behaviour that falls below the standards expected by the School.

Such incidents may be managed in accordance with the Behaviour Policy, Staff Code of Conduct, Staff Disciplinary Procedures, Acceptable Use Policies or other relevant school procedures.

Inappropriate Content

Although the School maintains filtering and monitoring systems to help protect users from harmful content, no technical solution can eliminate risk entirely.

If inappropriate, harmful or potentially illegal content is encountered on the School's systems or network, it must be reported immediately to the DSL and the Group Director of ICT. Appropriate action will then be taken to safeguard individuals, secure evidence where necessary and review any technical safeguards.

Support and Education

The School's response to online safety incidents will take account of the age, understanding and circumstances of those involved. Wherever appropriate, responses will include education, support and restorative approaches alongside any necessary sanctions or disciplinary measures.

Online safety concerns will be managed consistently with the School's Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct and Acceptable Use Policies.