Online Safety Policy

This policy, which applies to the whole school, inclusive of boarding, is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the school Compliance Officer.

This policy and its efficacy are reviewed and updated annually (or more frequently when national guidance or institutional learning requirements demand it).

Owner: Deputy Head Pastoral

Approving Body: Safeguarding and Wellbeing Committee

Date of last Review: September 2026

Date of next Review: September 2027

Linked Polices, Procedures and Resource Materials:

- Safeguarding and Child Protection Policy
- Risk assessments for student welfare
- AI Policy
- Anti-bullying Policy
- Behaviour, Rewards and Sanctions Policy
- SEND Policy including Reasonable Adjustments
- Woldingham Handbook
- Parent Contract
- Plagiarism Policy
- PSHE Policy
- RSE Policy
- Acceptable Use Agreements
- Privacy Notice – Students, Parents and Alumnae
- Privacy Notice – Staff
- Privacy Notice - Recruitment
- Data Protection Policy
- Data Retention and Storage Policy
- Staff Handbook
- Technical Security Guidance
- Visitor and Visiting Speaker Policy

KEY CONTACTS

Governors	**Chair of Governors** Catharine Berwick EMAIL: berwickc@woldinghamschool.co.uk **Nominated Safeguarding Governors** Ifey Summers EMAIL: summersi@woldinghamschool.co.uk Nick Waite EMAIL: waiten@woldinghamschool.co.uk
Online Safety Governor	Nick Waite EMAIL: waiten@woldinghamschool.co.uk
The Head	**Mrs Sue Baillie** TEL: 01883 349431 EMAIL: head@woldinghamschool.co.uk
Designated Safeguarding Lead	**Joy Ugono –** Deputy Head Pastoral Tel: 01883 654251 Mob: 07514 800042 EMAIL: ugonoj@woldinghamschol.co.uk
Deputy Designated Safeguarding Lead Team	**DEPUTY DSL** **Mrs Abigail Eland** – Safeguarding Manager and Mental Health Lead TEL school hours: 01883654251 TEL out of school hours: 07514 800 042 EMAIL: elanda@woldinghamschool.co.uk **DEPUTY DSL** **Mme Marie Emery** – Head of Year 10 TEL school hours: 01883654099 TEL out of school hours: 07768812936 EMAIL: emerym@woldinghamschool.co.uk

	DEPUTY DSL **Mr Terry Nunes** – Assistant Head Co-curricular TEL school hours: 01883654179 TEL out of school hours: 07979903904 EMAIL: nunest@woldinghamschool.co.uk **DEPUTY DSL** **Mr Alex Sharkey** – Head of Wellbeing TEL school hours: 01883654357 TEL out of school hours: 07768856655 EMAIL: sharkeya@woldinghamschool.co.uk **DEPUTY DSL** **Mrs Pippa Whitby** – Assistant Head Boarding TEL school hours: 01883 654100 TEL out of school hours: 07768 853 414 EMAIL: whitbyp@woldinghamschool.co.uk **DEPUTY DSL – SCHOOL HOLIDAY CONTACTS** **Ms Liz Roche** – Director of Finance and Operations TEL: 01883654202 MOBILE: 07825436718 **Mr Paul Ireland** – Director of IT TEL: 01883654145 MOBILE: 07768776006 **Ms Jacqui Collins** – Head of Human Resources TEL: 01883654014 MOBILE: 07768703212

Online Safety Lead	**Paul Ireland** – Director of IT EMAIL: irelandp@woldinghamschool.co.uk

Table of Contents

KEY CONTACTS 1
DEFINITIONS 5
AIMS AND SCOPE 5
ACCEPTABLE USE AGREEMENTS 6
ONLINE SAFETY GROUP 6
REPORTING AND RESPONDING 7
Reinforcing Acceptable Use Expectations 8
ROLES AND RESPONSIBILITIES 9
EDUCATION, ENGAGEMENT AND TRAINING 13
- Vulnerable Students 15
SAFER USE OF TECHNOLOGY 16
Internet Access and Network Security 16
Filtering and Monitoring Online Activity 17
Appropriate filtering 17
Appropriate Monitoring 18
Use of School-owned and personal Devices 19
Cyber Security 20
Social media 20
APPENDIX 1 - RESPONDING PROCEDURES TO ONLINE CONCERNS 23
Online child-on-child abuse 23
Child-on-Child Sexual Violence and Sexual Harassment 23
Nude or semi-nude image sharing 24
Cyberbullying 26
Online child abuse 27
Grooming, child sexual exploitation (CSE) and child criminal exploitation (CCE) 28
Indecent Images of children (IIOC) 28
Online Hoaxes and harmful online challenges 29
Online hate 30
Online radicalisation and extremism 30
Cybercrime 30
Staff, Governors or Volunteers 30
APPENDIX 2 - FLOWCHART FOR ACTION 31

DEFINITIONS

Staff –all staff, including the governing body, senior leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school

Students – All students on role at the School

Visitors – external contractors, visitors

Parents – Parents, carers, guardians, people with parental responsibility,

The School – Woldingham School

AIMS AND SCOPE

This policy takes into account DfE statutory guidance and local safeguarding children multi-agency partnership procedures.

Woldingham School ('the School') recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out a whole school approach to online safety which will empower, protect and educate students and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

The School understands that the breadth of issues classified within online safety is vast, but can be categorised into four areas of risk (as identified in KCSIE – currently in force):

- **content**: being exposed to illegal, inappropriate or harmful content (images and videos), for example: pornography, racism, misogynistic content, AI generated or 'deepfake' harmful material, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact**: being subjected to harmful online interaction with other users; for example: the risks arising from student use of AI chatbots and generative AI tools, 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**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The School recognises that children are at risk of abuse online as well as face to face; abuse can happen in school, out of school and in digital spaces. In many cases abuse will take place concurrently via online channels and in daily life. Child-on-child abuse can also occur online.

The School will ensure that students, staff and parents are supported in understanding emerging online risks, including misinformation, disinformation, deepfakes, AI-generated content, online scams and other evolving digital safeguarding concerns.

The School identifies that the internet and technology, including computers, tablets, mobile phones, other smart technology devices such as watches, games consoles and social media, are an important part of everyday life, and present positive and exciting opportunities, as well as challenges and risks.

This policy applies to all access to and use of technology, both on and off-site.

ACCEPTABLE USE AGREEMENTS

The school has defined what it regards as acceptable/unacceptable use and this is shown in the Acceptable Use Agreement (AUA).

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The key messages within the acceptable use agreements will be communicated/re-enforced through:

- Woldingham handbook
- Parent Portal
- staff induction and handbook
- splash screens
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website

The acceptable use agreements can be requested from the Compliance Officer.

ONLINE SAFETY GROUP

The school's Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group is made up of a combination of the following members:

- Deputy Head Pastoral/DSL (Co-Chair)
- Director of IT/ Online Safety Lead [OSL] (Co-Chair)
- Assistant Head Boarding
- Online Safety Governor
- IT and Cyber Security Manager
- Head of PSHE
- Compliance Officer

Members of the Online Safety Group will assist the DSL/OSL with:

- the reviewing and monitoring of the school Online Safety documents
- the reviewing and monitoring of the school filtering policy and requests for filtering changes

- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of students to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

While the responsibility for online safety is held by the DSL and cannot be delegated, the school has appointed an Online Safety Lead (OSL) to work in support of the DSL in carrying out these responsibilities. There is considerable emphasis on bringing together the safeguarding expertise of the DSL and the IT expertise of the Director of IT to ensure students stay safe at school.

REPORTING AND RESPONDING

The School will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking - offences under the Computer Misuse Act
    - Copyright theft or piracy
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss

- where there is no suspected illegal activity, devices may be checked in line with the searching and confiscation procedure outlined in the school's Behaviour, Rewards and Discipline Policy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors according to the school's Safeguarding and Child Protection Policy
- that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on CPOMs to provide a record
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions where appropriate.
- learning from the incident (or pattern of incidents) will be provided as relevant and anonymously, as appropriate, to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *students, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant*

Reinforcing Acceptable Use Expectations

The School have commenced a rollout of school issued student devices to Year 7 and 10 (September 2026). This enables the management of all aspects of the device ensuring content can only be accessed through the school filtering and monitoring systems and prevent the installation and use of any unauthorised/inappropriate software (e.g. VPNs).

Students own devices are required to be logged onto the school's network using the student's network credentials, then the installation of Securly certificate is required to allow internet access through the schools filtering and monitoring system, this applies to day girls and boarders at all times.

The School has a clear and proportionate approach to managing the risks presented by boarders' access to harmful online content, including where this may be accessed or stored on personal devices and through mobile data connections (3G, 4G and 5G) that bypass the school's filtering and monitoring systems. All boarders' devices are subject to the school's acceptable use and boarding rules, including requirements for registration on entry to the boarding environment and restrictions on use in identified high-risk contexts, such as unsupervised use overnight as outlined in the school Boarding Care Policy.

The school takes appropriate steps to reduce the risk of harmful content being brought into or accessed within the boarding environment, including where such content may already be downloaded onto a device. In Boarding Houses staff are professionally curious when students are using their devices, talking to them about what they are viewing/accessing and encouraging open dialogue about safety online including accessing content that might not present initially as harmful but that could be.

Where there is a safeguarding concern, the school will take proportionate action in line with statutory guidance; this may include the confiscation and examination of devices by authorised staff, with the involvement of the safeguarding team and, where appropriate, external agencies. This is in accordance with the school's Searching and confiscation guidance within the Behaviour, Rewards and Discipline policy.

This approach is supported by staff training, effective supervision, including in boarding, and a curriculum that promotes understanding of online safety and responsible technology use. Students are encouraged to report concerns, and all incidents are managed in accordance with the school's safeguarding procedures, with appropriate oversight by senior leaders.

The school recognises that boarding is a home away from home environment and the use of devices will be different than in a classroom setting. Boarding staff therefore actively supervise device use in line with published expectations (e.g. Woldingham Handbook and AUA), and routine procedures (including device registration and, where appropriate, managed access and overnight restrictions – see Mobile Phone and BYOD Policy) are applied consistently. Staff understand the action to take where concerns arise about harmful online content, including content already stored on a device or accessed through mobile data, and report such concerns promptly to the DSL and Assistant Head Boarding. Boarders confirm through discussion that they understand the school's expectations, the risks associated with unfiltered internet access, and how to report concerns.

Records are maintained on CPOMS of any incidents involving inappropriate or harmful content, including actions taken and outcomes, and are reviewed by senior leaders (including the DSL) to identify patterns or emerging risks. The effectiveness of this approach is monitored through safeguarding reviews e.g. within the online safety group, staff training updates and oversight by governors, ensuring that practice remains responsive to evolving risks associated with technology.

ROLES AND RESPONSIBILITIES

Governors are responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Ensuring their own knowledge of online safety issues is up to date by undertaking training.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with IT staff and service providers.

- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges' filtering and monitoring standards.

The Head is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL Team by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Recruitment: as part of the shortlisting process, consider carrying out an online search as part of their due diligence on shortlisted candidates to help identify any incidents or issues that have happened, and are publicly available online which the school/ academy might want to explore with applicants at interview.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility working closely with the Online Safety Lead for online safety in the school.
- Understanding the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the Learning Enhancement and IT support staff.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff, and ensuring all members of the school community understand this procedure.
- Alongside the Director of IT, understanding and taking responsibility of the filtering and monitoring processes in place at the school.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping students safe.
- Communicate regularly with parents to reinforce the importance of children being safe online.

- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.

The Director of IT (Online Safety Lead) is responsible for:

- Promoting online safety and the adoption of a whole school approach.
- Embedding appropriate support for staff to use the internet safely with their students.
- Carrying out risk assessments on effectiveness of filtering systems.
- Auditing and evaluating online safety practice.
- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Maintaining filtering and monitoring systems.
- Providing filtering and monitoring reports.
- Completing actions following concerns or checks to systems.

The School's service provider, in partnership with the senior leadership team and DSL are responsible for:

- procuring systems
- identifying risk
- carrying out reviews
- carrying out checks

The School carries out all the online safety measures that its obligations and responsibilities require. The Provider follows and implements this policy and its procedures and is responsible for ensuring that:

• They are aware of and follow the School Online Safety Policy to carry out their work effectively in line with School policy

• The School's technical infrastructure is secure and is not open to misuse or malicious attack. Servers, wireless systems and cabling must be securely located and physical access restricted and individual workstations are protected by up-to-date virus software

• The School meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority

• There is clear, safe, and managed control of user access to networks and devices

• They keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others

• The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL

• Requests from staff for sites to be removed from the filtered list will be considered by the Director of IT in discussion with the DSL as appropriate.

• Monitoring systems are implemented and regularly updated as agreed in School policies

• Systems are in place to regularly monitor and record the activity of users of the school IT systems and users are made aware of this in the Acceptable Use Agreement.

• Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges (and others outlined in local authority / MAT policy and guidance). Further information can be found within the School's Technical Security guidance.

All staff members are responsible for:

• The security of IT systems and electronic data they use or have access to.

• Modelling good online behaviours.

• Maintaining a professional level of conduct in their personal use of technology.

• Having an awareness of online safety issues.

• Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.

• Reporting concerns in line with the school's reporting procedure.

• Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum

Students are responsible for:

• Adhering to the Acceptable Use Agreement and other relevant policies.

• Seeking help from school staff if they are concerned about something they or anyone else has experienced online.

• Reporting online safety incidents and concerns in line with the procedures within this policy

Students are responsible for:

- Signing the student Acceptable Use Agreement at the beginning of each academic year
- Using the school digital technology systems in accordance with the student acceptable use agreement and Online Safety Policy (this includes personal devices – where students have permission to use them)
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Knowing what to do if they or someone they know feels vulnerable when using online technology.

- Understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school or on their school issued device.

Parents are responsible for supporting the School by:

- Countersigning the student Acceptable Use Agreement at the beginning of each academic year
- Playing a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way
- Reinforcing the online safety messages provided to students in school.
- Encouraging the safe and responsible use of their children's personal devices in and out of the school

The School will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- requiring them to countersign the students' acceptable use agreement
- publishing information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital data including images and cloud services
- newsletters, website, social media and information sessions about national/local online safety campaigns and literature.

Community users are responsible as follows:

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

EDUCATION, ENGAGEMENT AND TRAINING

Students

The School references the DfE 'teaching online safety in schools' guidance during the creation of their curriculum. Online safety is embedded throughout the curriculum and teaching is always appropriate to students' ages and developmental stages. All students will be taught about online safety as part of the curriculum in accordance with the government's guidance on relationships and sex education (RSE) 2025. Students are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours students learn through the curriculum include the following:

• How to evaluate what they see online

• How to recognise techniques used for persuasion

• Acceptable and unacceptable online behaviour

• How to identify online risks

• How and when to seek support

• Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks students may face are always considered when developing the curriculum. The School's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring students develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

The School

The School will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from students.

This will be provided through:

- PHSE, Thrive and RSE programmes
- through pastoral avenues, eg assemblies
- through relevant national initiatives and opportunities e.g. *Safer Internet Day* and *Anti-bullying week.*

The DSL is involved with the development of the school's online safety curriculum. Students will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Key staff members will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

Relevant members of staff, e.g. the Learning Enhancement Team and DSL will work together to ensure the curriculum is tailored so that students who may be more vulnerable to online harms, e.g. students with SEND and DSL, receive the information and support they need.

Teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students.

Before conducting a lesson or activity on online safety, the teacher considers the topic that is being covered and the potential that students in the class have suffered or may be suffering from online abuse or harm in this way. The DSL or wider pastoral team may be required to advise the staff member on how to best support any student who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which students feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything students raise during online safety lessons and activities, or if a student makes a disclosure regarding online abuse following a lesson or activity, they will make a report in line with the School's Safeguarding and Child Protection Policy.

- **Use of technology in the classroom and beyond including students in boarding and learning remotely**

A wide range of technology is used in classrooms, in boarding environments and at home when necessary, including but not limited to the following:

- Laptop/Desktop Computers
- Mobile/Tablets/Smart Technology Devices
- Internet and Email
- Photo/Video/Audio equipment
- Learning platforms, remote learning platforms
- Games consoles and other gaming technologies

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher always review and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law. Students are supervised when using technology and/or online materials during lesson time – this supervision is suitable for their age and ability. Use of video sharing platforms will be in accordance with the school's IT terms of use, following a risk assessment and with appropriate safety and security measures in place.

- **Vulnerable Students**

Woldingham School recognises that any student can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some students, for example children with special educational needs or disabilities or gender questioning children, who may be more susceptible or may have less support in staying safe online. The School will endeavour to ensure that differentiated and appropriate online safety education, access and support is provided to all students who require additional or targeted support. Staff will seek input from specialist staff as appropriate, including the DSL and SENCO, to ensure that the policy and curriculum is appropriate to the students' needs.

Staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems.

All staff will be made aware that students are at risk of abuse (including child-on-child abuse) and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support students in developing critical thinking skills and safe online behaviours. Teaching staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

Parents

The School will work in partnership with parents to ensure students stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

• Child sexual abuse, including grooming.

• Exposure to radicalising content.

• Sharing of indecent imagery of students, e.g. sexting.

• Cyberbullying.

• Exposure to age-inappropriate content, e.g. pornography.

• Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content. Parental awareness regarding how they can support their children to be safe online is raised by the school via various methods which may include:

• Letters and newsletters

• School website and links to external online resources, e.g. the Wellbeing Hub on the Parent Portal, Child Exploitation and Online Protection Command (CEOP)

• High profile events, such as Safer Internet Day and Internet Safety Week

• Parent Webinars

• Information evenings

SAFER USE OF TECHNOLOGY

Internet Access and Network Security

Woldingham School does all it can to monitor access to the internet via the School network. Access to the School internet has been designed expressly for the use of students and includes filtering appropriate to their ages. The School uses Securly, a filtering system that blocks sites that fall into categories such as

self-harm, substance abuse, pornography, racial hatred, extremism, and other sites of an illegal nature or containing material unsuitable for children. No device, whether School owned or personal, can meaningfully access the internet through the School's system without going through the filtering system. Access to the internet for students and staff is governed by the frameworks outlined in the Acceptable Use Agreements with clear guidelines about student and staff behaviour in relation to the internet and the use of the School network. The security of the School information systems will be reviewed regularly, and virus protection is updated on a regular basis.

Students, staff and other members of the school community including visitors are only granted access to the school's internet network once they have read and agreed to an Acceptable Use Agreement. All students are required to use the school's network whilst on site as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately for their age group.
Use of VPNs to bypass these systems is recognised as a breach of the Acceptable Use Agreement and followed up as appropriate. Staff, residents and visitors are also encouraged to use the school network on a 'WoldGuest' network which has appropriate filtering and monitoring. The password for the 'WoldGuest' network should not be shared with students under any circumstances.

Filtering and Monitoring Online Activity

Woldingham School follows guidance published by the UK Safer Internet Centre, as well as the Department for Education's filtering and monitoring standards, to ensure that it maintains appropriate filtering and monitoring provision. Key staff such as the Online Safety Group are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

Appropriate filtering

- a member of the SLT and a governor, are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined
- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre *Appropriate filtering.*
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes

- filtering logs are regularly reviewed and alert the DSL to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings. (Schools may wish to use e.g. using SWGfL Testfiltering.com to carry out these checks)
- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/students, etc.)
- the school has a Mobile Phone and BYOD policy and where personal mobile and other smart technology devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice. (schools should be aware of the difficulties of providing effective filtering on some tablet devices)

If necessary, the school will seek advice from, and report issues to, the SWGfL *Report Harmful Content* site.

Appropriate Monitoring

The school follows the UK Safer Internet Centre *Appropriate Monitoring* guidance.

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices.

Emails – Students are inducted into the appropriate use of e-mail and there is clear guidance in the Woldingham Handbook and Staff Handbook about acceptable communication. Any inappropriate email must be reported immediately to Director of IT and to the DSL where appropriate.

Generative Artificial Intelligence – The School's AI Policy outlines clear guidance on the use of such technologies in the school.

Social Networking - Access to social networking sites is filtered as appropriate. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times. Staff are not permitted to communicate with students or parents over social networking sites in an official capacity and are reminded to alter their privacy settings to ensure students and parents are not able to contact them on social media.

Students are taught how to use social media safely and responsibly through the online safety curriculum. Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.

The School Website - The Head and the Director of External Communications are responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and students is not published on the website.

Use of School-owned and personal Devices - Staff members may be issued with devices such as laptops, tablets, mobile phones etc to assist with their work. Students are required to have a device as necessary to assist in the delivery of the curriculum. All devices using the school network are used in accordance with the acceptable use agreements.

IT staff monitor school-owned devices and assist with personal devices using the school network. School-owned devices are automatically installed with software updates and antivirus definitions. No software, apps or other programmes can be downloaded onto a school-owned device without authorisation from IT support staff. Cases of staff members or students found to be misusing school-owned devices will be managed in line with the Behaviour, Rewards and Sanctions Policy or Staff Handbook as appropriate.

Mobile Phones

The School recognises that the majority of students have mobile phones with unrestricted access to digital spaces via 3G, 4G and 5G. As such, Woldingham School has a Mobile Phone and BYOD policy promotes a mobile phone-free environment to support focused learning, positive social interaction, and student wellbeing throughout the school day. To reinforce this, Years 7-11 groups are required to be completely mobile phone-free during the school day, with clear expectations also outlined in the Woldingham Handbook.

Where a student uses accessibility features on a personal device to help them access education, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

Cyber Security

In the light of the very real risks of a cybersecurity breach occurring at the School:

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, (*in partnership with their technology support partner),* has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school's education programmes include cyber awareness for students
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents.

All students and staff have a responsibility to report cyber risk or a potential incident or attack. The School ensures staff understand how to do this and feel safe and comfortable to do so.

Social media

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for students, parents/carers

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.

- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

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

- a process for approval by senior leaders led by the Director of External Communications
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with where there is cause for concern in relation to safeguarding members of the school community.

School use of social media for professional purposes will be checked regularly by a member of the SLT and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

All images of students used in official external school promotional materials will be altered using AI technology to safeguard students as best as possible. – refer to Taking, Storing and Using Student Images Policy.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the School are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of public social media

- As part of active social media engagement, the School may pro-actively monitor the internet for public postings about the school.
- the school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media, they will be urged to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Review of job applicants and visiting speaker social media

Job applicant and visiting speaker social media will be reviewed by the School as necessary in order to ensure the safety and wellbeing of the students. Further details can be found in the Privacy notice – Recruitment and the Visitor and Visiting Speaker Policy.

APPENDIX 1 - RESPONDING PROCEDURES TO ONLINE CONCERNS

Online child-on-child abuse

Child-on-Child Sexual Violence and Sexual Harassment

When responding to concerns relating to online child on child sexual violence or harassment, the School will follow the guidance outlined in Part Five of KCSIE, as well as being mindful of Childnet's online sexual harassment guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-forschools-and-professionals

Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.

All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.

The School recognises that sexual violence and sexual harassment between children can take place online. Examples may include:

- consensual and non-consensual sharing of nude and semi-nude images and videos
- sharing of unwanted explicit content
- 'upskirting' (which is a criminal offence and typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
- sexualised online bullying
- unwanted sexual comments and messages, including, on social media
- sexual exploitation, coercion and threats.

The School recognises that sexual violence and sexual harassment occurring in digital spaces (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms, and for things to move from platform to platform online.

Concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took on or offline will be dealt with according to the Safeguarding and Child Protection Policy. The School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment and the support available, by implementing a range of age and ability appropriate educational methods as part of the curriculum. When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator and any other children involved/impacted.

The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children and staff and any actions that are required to protect them.

Reports will initially be managed internally by the DSL, including where appropriate seeking advice from the Education Safeguarding Service, and where necessary will be referred to Children's Social Care and/or the Police.

The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.

If content is contained on students' personal devices, they will be managed in accordance with the School's Behaviour, Rewards and Discipline Policy and DfE 'searching screening and confiscation' advice.

Following an immediate risk assessment, the school will:

- provide the necessary safeguards and support for all students involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
- inform parents for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
- if the concern involves children and young people at a different educational school, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community. If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised.
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Woldingham School recognises that the internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. The School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online

Nude or semi-nude image sharing

The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex.

Woldingham School recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue and all concerns will be reported to and dealt with by the DSL.

This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:

- creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
- shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
- possesses nude and/or semi-nude imagery created by another person (or AI created image) under the age of 18.

When made aware of concerns regarding nude and/or semi-nude imagery, staff will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

Staff will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods.

The School will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.

When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:

- Report any concerns to the DSL immediately.
- Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, they must be immediately report this to the DSL.
- Not delete the imagery or ask the child to delete it.
- Not say or do anything to blame or shame any children involved.
- Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
- Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

If made aware of an incident involving nude or semi-nude imagery, DSLs will:

- act in accordance with our Safeguarding and Child Protection Policy and the relevant local procedures and in line with the UKCIS guidance.
- carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of students involved, including the possibility of carrying out relevant checks with other agencies.
- make a referral to Children's Social Care and/or the police immediately if:
- the incident involves an adult (over 18).

- there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
- the image/videos involve sexual acts and a child under the age of 13, depIT sexual acts which are unusual for the child's developmental stage, or are violent.
- a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
- consider whether to involve other agencies at any time if further information/concerns are disclosed at a later date .
- seek advice from the Education Safeguarding Service if unsure how to proceed.
- store any devices securely:
- If content is contained on students' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
- provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
- implement sanctions where necessary and appropriate in accordance with our Behaviour Policy but taking care not to further traumatise victims where possible. o consider the deletion of images in accordance with the UKCIS guidance.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
- Students will be supported in accessing the Childline Report Remove tool for nude images where necessary o review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Staff will not:

- view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, and any decision making will be clearly documented.
- send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request students to do so

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

• Threatening, intimidating, discriminatory or upsetting messages

• Threatening or embarrassing media sent via electronic means

• Silent or abusive phone calls or using the victim's device to harass others, to make them think the victim is responsible

• Unpleasant or defamatory information/comments/messages posted online

• Abuse between young people in intimate relationships online.

The school will be aware that certain students can be more at risk of abuse and/or bullying online, such as LGBTQ+ students and students with SEND. Cyberbullying with regard to the protected characteristics according to the Equalities Act 2010 is particularly serious.

Cyberbullying against students or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy

Online child abuse

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

• Threatening, facilitating or encouraging sexual violence

• Voyeurism and Upskirting

• Sexualised online bullying

• Unwanted and unsolicited sexual comments and messages

• Consensual or non-consensual sharing of sexualised imagery

• Abuse between young people in intimate relationships online

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to students becoming less likely to report such conduct. Staff will be aware that creating, possessing, and distributing indecent imagery of children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves. The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other students taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Safeguarding and Child Protection Policy.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

Grooming, child sexual exploitation (CSE) and child criminal exploitation (CCE)

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them. Staff will be aware that grooming often takes place online and that students who are being groomed are commonly unlikely to report this behaviour for many reasons. Due to the fact students are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including but not limited to:

• Being secretive about how they are spending their time.

• Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

• Having money or new possessions, that they cannot or will not explain.

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation. CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet. Where staff have any concerns about students with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Indecent Images of children (IIOC)

Woldingham School will:

- ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.
- respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and antispam software.
- obtain advice immediately through the police and/or the Education Safeguarding Service if it is unclear that a criminal offence has been committed.

If made aware of IIOC, the School will:

- act in accordance with our Safeguarding and Child Protection Policy and the relevant local safeguarding children partnership procedures.

- store any devices involved securely, until advice has been sought.
- Never view the IIOC

If content is contained on students' personal devices, they will be managed in accordance with the School Behaviour, Rewards and Discipline Policy and DfE 'searching screening and confiscation' advice.

- immediately inform appropriate organisations, such as the IWF and police.

If made aware that a member of staff or a student has been exposed to indecent images of children, staff will:

- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses), which contain the suspect images, are reported appropriately eg. to the IWF via www.iwf.org.uk and/or police.
- inform the police as appropriate, for example if images have been deliberately sent to or shared by students. o report concerns as appropriate to parents and carers.

If made aware that indecent images of children have been found on school provided devices, staff will:

- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses), which contain the suspect images, are reported appropriately, eg to the IWF via www.iwf.org.uk .
- inform the police via 101 or 999 if there is an immediate risk of harm, and any other agencies, such as children's services, as appropriate.
- only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
- report concerns, as appropriate to parents/carers.

If made aware that a member of staff is in possession of indecent images of children, staff will:

- ensure that the Head is informed in line with our policy on managing allegations against staff.
- inform the LADO and other relevant organisations, such as the police.
- quarantine any involved school provided devices until police advice has been sought.

Online Hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms. For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the student and the way in which they are depicted in the video. Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the school, they will report this to the DSL immediately. The DSL will conduct a case-by-case assessment for

any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students. The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible

Online hate

Online hate content, directed towards or posted by specific members of the community will not be tolerated at Woldingham School and will be responded to in line with existing policies, including Safeguarding and Behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The police will be contacted if a criminal offence is suspected. If staff are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Local Authority and/or the police.

Online radicalisation and extremism

The School will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site. If staff are concerned that a student may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Safeguarding and Child Protection Policy

Cybercrime

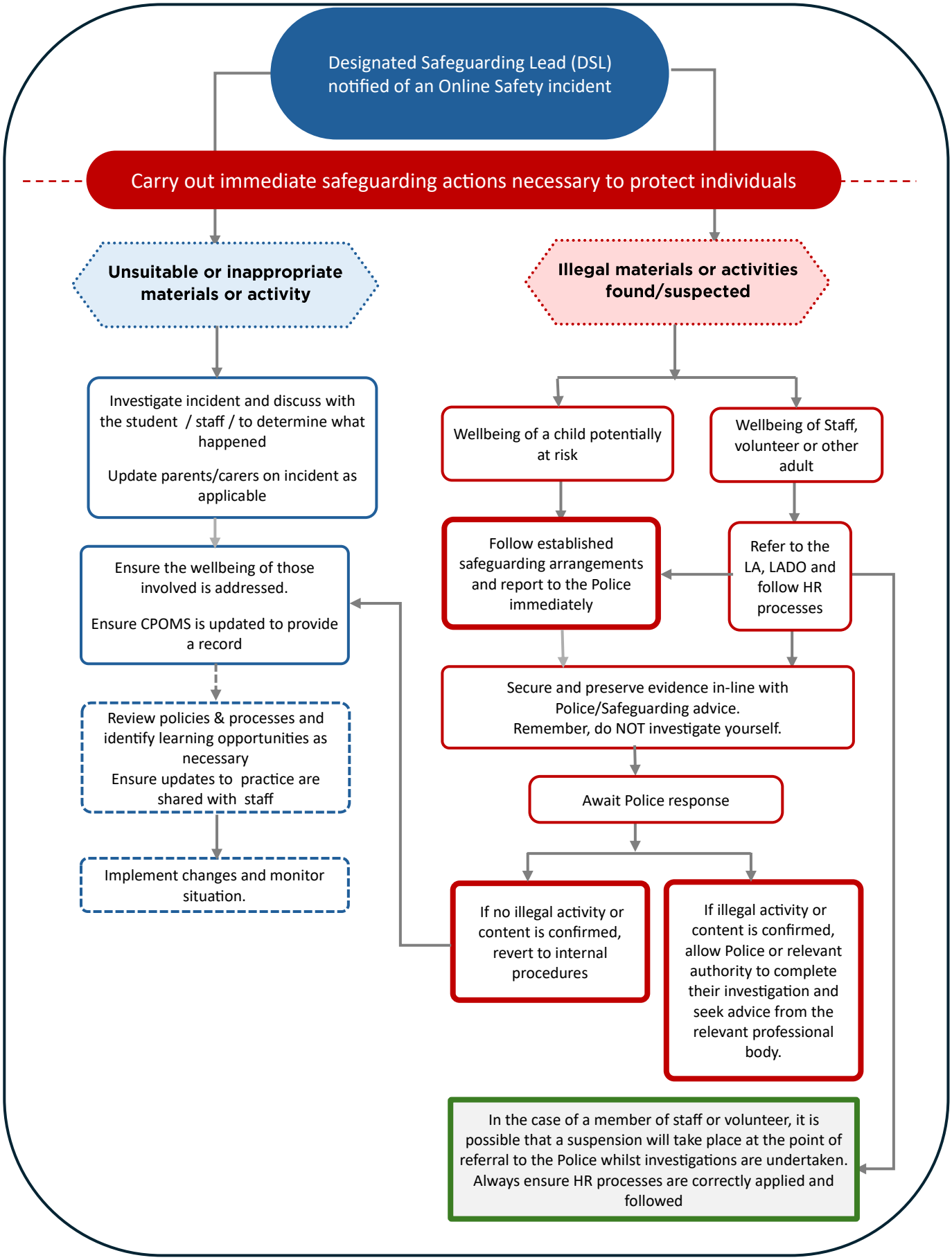
Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

• Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

• Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests. The DSL and headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully

Staff, Governors or Volunteers

Any concerns regarding the online behaviour of members of staff, governors, other volunteers or visitors at the School must be reported and dealt with according to the School Safeguarding and Child Protection Policy.

APPENDIX 2 - FLOWCHART FOR ACTION