Policy No: 7h

WOLDINGHAM SCHOOL

ONLINE SAFETY POLICY INCLUSIVE OF CYBER BULLYING, ACCEPTABLE USE AND SOCIAL MEDIA

This policy applies to the whole school including boarding

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 Office.

Document Details

Information Sharing Category	Public Domain
Version	3
Date Published	September 2022
Authorised by (if required)	The Head and Board of Governors
Responsible Area	Safeguarding Team

Availability: All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours, including activities away from school. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the Policies Register.

Monitoring and Review: This document will be subject to continuous monitoring, refinement and audit by the Head. This document was reviewed and agreed by the Board of Governors in September 2022 and if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require, prior to September 2022, the policy will be reviewed accordingly.

Signed: Reviewed: September 2022

Next Review: September 2023

Dr James Whitehead
Head

Mr Robert Parkinson
Chair of Governors

Introduction: The purpose of this Policy is to safeguard students and staff at Woldingham School. It details the actions and behaviour required from students and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements we have a whole school approach to Online Safety. Our key message to keep students and young people safe is to be promoted and should be applied to both online and offline behaviours. Within our Online Safety policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding & Child Protection Policy and other related documents.

Online safety is a running and interrelated theme when devising and implementing our wider school policies and procedures, including our Safeguarding & Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy. The staff and student Acceptable Use Policies (AUPs) are central to the Online Safety policy and should be consulted alongside this policy. We consider how we can promote online safety whilst developing our curriculum, through our staff training, and also through parental engagement. The Online Safety policy will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies. The Student Council will be consulted regarding any changes to the Student AUP. All staff should read these policies in conjunction with the Online Safety policy. This is particularly important with regard to the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Safeguarding & Child Protection and Preventing Extremism and Tackling Radicalisation Policies.

Roles and Responsibilities: Our nominated Online Safety Officer is the DSL who has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice; this role overlaps with that of the Designated Safeguarding Lead.
Their roles will include ensuring:

- Young people know how to use the Internet responsibly and that parents and teachers have the right measures in place to keep students safe from exploitation or radicalisation.
- Students are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- To ensure that students use Information and Communications Technology (ICT) safely and securely and are aware of both external and peer to peer risks when using ICT, including cyberbullying and other forms of abuse.
- All staff and volunteers will receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- The Acceptable Use Policy (AUP) is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be transparent and updated as agreed in school policies.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- An appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- A current record of all staff and students who are granted access to school ICT system is maintained.

Designated Safeguarding Lead (DSL): The Designated Safeguarding Lead (DSL) is a senior member of the management team who has relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is available at all times, for example, a Deputy Designated Safeguarding Lead is also in place should the DSL be absent. The designated persons for safeguarding will be responsible for ensuring:

- Agreed policies and procedures are to be implemented in practice.

- All updates, issues and concerns are to be communicated to all ICT users.
- The importance of online safety in relation to safeguarding is to be understood by all ICT users.
- The training, learning and development requirements of staff are to be monitored and additional training needs identified and provided for boarding specific training.
- An appropriate level of access authorisation is given to ICT users.

Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures. The learning and development plans of students and young people will address online safety. A safe ICT learning environment is to be promoted and maintained.

The Board of Governors' responsibilities: Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the Board of Governors will do all that they reasonably can to limit children's exposure to risks when using the school's IT system. As part of this process, the Board has ensured the school has appropriate filters and monitoring systems in place which are reviewed regularly to monitor their effectiveness. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place, how to manage them effectively and know how to escalate concerns when identified.

All Staff: It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate internet access or use, both inside and outside of Woldingham School, and to deal with incidents of such as a priority. All staff are responsible for ensuring they are up to date with current Online Safety issues, and this online Safety Policy. Cyber-bullying incidents will be reported in accordance with Woldingham School's Anti-Bullying Policy. All staff will ensure they understand and adhere to our staff Acceptable Use Policy, which they must sign and return to the online Safety Officer and a copy placed on staff file. Teachers will ensure they are confident in delivering the school's computing and Online Safety curriculum as required, identifying risks and reporting concerns as they arise.

Parents: Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately. Woldingham School will support parents by sharing information and links through newsletters, school's website, Facebook feeds, Microsoft Teams and informal/formal training.

All Students: All students will ensure they understand and adhere to our student Acceptable Use Policy, which they must sign and return to the Online Safety Officer. Students are reminded of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

Breadth of Online Safety Issues: We classify the issues within online safety into **four** areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; 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:** 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; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

These issues are to be managed by reducing availability, restricting access, promoting safe and responsible use.

Staff/Volunteers Use of IT Systems: Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the 'Staff Code of Conduct for ICT) (please see appendices) before using any school ICT resource. In addition:

- All staff, including the Board of Governors, will receive annually updated Online Safety training.
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password-protected computers and other devices. Staff are advised to follow the "How do I stay secure on the Internet?" section in the Online Safety FAQ document.
- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the students visit.
- Occasionally students may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study. Every request to do so should be auditable with clear reasons for the need.
- The Internet can be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved web browsers and email systems which have appropriate security in place. Additionally, files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes.
- Additionally, staff should not communicate with students through electronic methods such as social networking sites, blogging, chat rooms, texts or private email. Instead, only the school email system should be used for this purpose.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e. videos of lessons, activities, or fieldtrips, should be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the school's Online Safety Officer.
2. The Online Safety Officer should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the CEOP or the police will be informed.
5. No student or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

Teaching about online safety: Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. Online Safety is a focus in all areas of the curriculum and key Online Safety messages are reinforced regularly, teaching students about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Access levels to ICT reflect the curriculum requirements and age of students. Staff should guide students to on-line activities that will support the learning outcomes planned for the students' age and maturity. This teaching is built into existing lessons alongside our wider whole-school approach. Students will explicitly be taught the following topics through their lessons:

- What internet use is acceptable and what is not and given clear guidelines for internet use;
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications;
- How to evaluate what they see online;
- How to recognise techniques used for persuasion;
- Online behaviour;
- How to identify online risks and
- How and when to seek support.

We recognise that Peer-on-Peer abuse can occur online and to this end we teach students how to spot early warning signs of potential abuse, and what to do if students are subject to sexual harassment online. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying

- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, eg involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Staff should be vigilant in lessons where students use the Internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with school policy. Staff will be provided with sufficient Online Safety training to protect students and themselves from online risks and to deal appropriately with Online Safety incidents when they occur. Ongoing staff development training includes training on online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements.

Harmful online challenges and online hoaxes: (Please refer to the latest DfE Guidance) There has been a growing trend in the number of both challenges and hoaxes online as well as their popularity. As such, the school has put in a number of measures to safeguard our children. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We teach pupils to recognise the signs that something may be untruthful online or that risks associated with any online challenges as well as who they can speak to if they have a concern. Where a child or member of staff reports an online hoax or challenge, we ensure that they are taken seriously, and acted upon appropriately, with the best interests of the child coming first. We ensure we provide opportunities to discuss this topic within Online Safety lessons, ensuring children and young people can ask questions and share concerns about what they experience online without being made to feel foolish or blamed.

A case-by-case assessment, establishing the scale and nature of the possible risk to our students will be carried out, and appropriate actions taken, which may include sharing information with parents and carers, our own young people as well as other local schools. Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion by spreading information which itself is untrue or would only draw students' attention to a potential risk.

Our DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful. Information that is shared with parents and carers will include encouraging them to focus on positive and empowering online behaviours with their children, such as critical thinking, how and where to report concerns about harmful content and how to block content and users.

Students Use of IT Systems: All students must agree to the IT Acceptable Use Policy before accessing the school systems. Students at Woldingham School will be given supervised access to our computing resources and will be provided with access to filtered Internet (see FAQ Document) and other services operating at the school. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of students and young people. The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law. Woldingham School will help students to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially students, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, Social, Health and Economic Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- Teaching Online Safety in School https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- PSHE Association (https://www.pshe-association.org.uk/)
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

Educating Staff: A planned calendar programme of online safety training opportunities will be available to all **staff members, governors and volunteers** as part of CPD. Staff will be provided with sufficient Online Safety training to protect students and themselves from online risks and to deal appropriately with Online Safety incidents when they occur. Ongoing staff development training includes training in online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements. Staff will undergo online safety training annually/when changes occur basis to ensure they are aware of current online safety issues and any changes to the provision of Online Safety, as well as current developments in social media and the internet as a whole. All staff will employ methods of good practice and act as role models for young people when using the internet and other digital devices. All staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism. Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this online safety policy/social media policy/user agreement. The online safety officer will act as the first point of contact for staff requiring online safety advice.

Communicating and Educating Parents/Guardians in Online Safety: We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. For example, Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on School website). Parents will also be provided with a copy of the Pupil IT Acceptance Policy, and parents will be asked to sign it, as well as students. Woldingham School recognises the crucial role that parents play in the protection of their students with regards to online safety. The school organises an annual awareness session for parents with regards to Online Safety which looks at emerging technologies and the latest ways to safeguard students from inappropriate content. The school will also provide parents and carers with information through newsletters, web site and the parent portals. Parents and guardians are always welcome to discuss their concerns on Online Safety with the school, who can direct them to the support of our Online Safety Officer if required. Parents and carers will be encouraged to support the school in promoting good Online Safety practice.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) (currently in force). The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Students are encouraged to keep their personal data private as part of our Online Safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will act responsible for ensuring we have an appropriate level of security protection procedures in place, in order to safeguard systems, staff and learners and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Radicalisation and the Use of Social Media to Encourage Extremism: The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people;
- Confirming extreme beliefs;
- Accessing likeminded people where they are not able to do this off-line, creating an online community;
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Woldingham School has a number of measures in place to help prevent the use of social media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by students.
- Students, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*

Reporting of Online Safety Issues and Concerns Including Concerns Regarding Radicalisation: Woldingham School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding Online Safety should be made to the Online Safety Officer, who will review the issue and take the appropriate action. For students, they are taught to raise any concerns to their class teacher who will then pass this on to the Online Safety officer. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy.

Our Designated Safeguarding Lead (DSL) provides advice and support to other members of staff on protecting students from the risk of on-line radicalisation. Woldingham School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify students at risk of being drawn into terrorism, and to challenge extremist ideas, which can be used to legitimise terrorism. Staff safeguard and promote the welfare of students and know where and how to refer students and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Developing technologies, such as mobile phones with Internet access are not governed by the school's infrastructure and can bypass any and all security and filtering measures that are or could be deployed. We recognise the additional risks this has for our students in boarding, who could have unsupervised access to the internet when using their own devices in their free time. To address this, the school works with pupils across our age range to ensure that students are educated clearly about the risks of both social media and internet use, alongside regularly monitoring of device usage as appropriate.
- We will audit ICT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Board of Governors will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered *Wi-Fi* access.
- Woldingham School takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard students from potentially harmful and inappropriate material on-line without unreasonable "over-blocking"
- The school recognises that students may choose to circumvent certain safety precautions by using mobile data on their devices over 3G, 4G and 5G. To help provide a safe environment for all students, we will supplement the systems filtering with behaviour management and additional staff/student training.

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets; please see appendix 3 for more details): Mobile telephones are permitted both in boarding houses and in academic school buildings. During the school day phones are only to be used by students during break time and lunch time, unless in the boarding houses.. Students must ensure that their devices are kept in a secure place, e.g. their school bag or in their locker. Mobile devices are kept on site at the risk of the individual student and Woldingham School is not responsible for any devices lost or damaged by students.

Recordings made using mobile electronic devices: Using the camera on a phone or similar device, either to photograph/film/record any member of the school community, do any form of live streaming or to show to others the photos/videos/audio recordings already on the phone or similar device is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied.

Cyber-Bullying: is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Cyberbullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection procedures (see our Safeguarding & Child Protection Policy).

Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;
- **Chat room bullying and online grooming** involve sending menacing or upsetting responses to students or young people when they are in a web-based chat room;
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where students and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, Group Me, Skype, Facebook Messenger, Snapchat, Google Hangouts etc.) as they conduct real-time conversations online;
- **Bullying via websites and social networks (an example of this would be Facebook, Twitter, Instagram, etc.)** includes the use of defamatory blogs, personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

What has Research into Cyber Bullying Found?

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyber-bullying is done by students in the same class or year group and although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

- Between a fifth and a quarter of students have been cyber-bullied at least once over the previous few months.
- Phone calls, text messages and email are the most common forms of cyber-bullying.
- There is more cyber-bullying outside school than in school.
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone.
- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying.
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying.
- Website and text bullying are equated in impact to other forms of bullying.
- Around a third of those being cyber-bullied tell no one about the bullying.

Students should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

Online Sexual Harassment: Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence. online sexual harassment include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, is unacceptable and will dealt with under our Child Protection Procedures.

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline 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 services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

a. The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. Providing expert advice and support for school staff with regard to online safety issues and when an allegation is received.
b. If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

ICT-Based Sexual Abuse (Including Sexting): The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with students, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Pupils are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

There are no circumstances that will justify adults possessing indecent images of students. Adults who access and possess links to such websites will be viewed as a significant and potential threat to students. Accessing, making and storing indecent images of students is illegal. This will lead to criminal investigation and the individual being barred from working with students, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with students. Adults should ensure that students are not exposed to any inappropriate images or web links. Where indecent images of students or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Sanctions: Sanctions will depend on the severity of the offence as assessed by the Senior Leadership Team. They may include one or more of the following:

- Temporary or permanent ban on the use of ICT resources in the School.
- Temporary or permanent ban on the use of the Internet in the School.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- Temporary or permanent exclusion from school may be imposed.
- If appropriate, police or local authorities may be involved.

Chat Room Grooming and Offline Abuse: Our staff need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of students online is a faster process than usual grooming, and totally anonymous. The abuser

develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Social Media, including Facebook, Twitter and Instagram: Facebook, Twitter, Instagram and other forms of social media are increasingly becoming an important part of our daily lives, including part of the school's marketing strategy.

- Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Head for reasons of work
- Staff are advised not to befriend or follow parents of students and to keep their personal profile as private as possible
- Staff and students are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff and students, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

Staff and students are aware that their online behaviour should at all times be compatible with UK law. Additionally, more information on best practice for staff can be found in our Staff Behaviour (Code of Conduct) Policy.
Woldingham School recognises that Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

Use of Email

- Pupils at KS3 and above will be provided with individual email addresses for educational use.
- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other young persons, staff or third parties via works email.
- Yong people are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages may be monitored.
- Any emails sent by young people to external organisations will be overseen by their teacher/support worker and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Taking and Storing Images of Students Including Mobile Phones (See our related documents including Appendix 3): Woldingham School provides an environment in which students, parents and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of students, or to take photographs of students apart from circumstances as outlined in Appendix 6 of this policy. This prevents staff from being distracted from their work with students and ensures the safeguarding of students from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a Mobile Phone Policy which includes:

- The commitment to keep the students safe.
- How we manage the use of mobile phones at Woldingham School, taking into consideration staff, students on placement, volunteers, other professionals, visitors and parents/carers.
- How we inform parents/carers, visitors and other professionals of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

Remote Learning (Please see our Remote Learning Policy for more details): Where there are periods in which the school is forced to close, yet continue to provide education (such as during the COVID-19 Pandemic) it is important that Woldingham School supports staff, students and parents to access learning safely, especially considering the safety of our vulnerable students. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns, and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Online teaching should follow the same principles as set out in the school's staff and pupils respective Behaviour - Code of Conducts. Additionally, school name will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The school will put additional measures in place to support parents and students who are learning from home. This will include specific guidance on which programmes the school is expecting students to use and how to access these alongside how students and parents can report any concerns that they may have. Guidance will also be issued on which staff members students will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our schools Remote Learning Policy.

Additionally, the Head has a duty of care for ensuring the safety (including online safety) of members of the school community, with the day to day responsibility being delegated to the Online Safety Lead who is our DSL. The Head and the DSL are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, which in line with our main safeguarding reporting procedures.

Staff working remotely should wherever possible use their school-issued ICT equipment, however they may use their own computer equipment if this is not practical, as long as it is in accordance with the school's Data Protection Policy. Staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

For more information relating to Online Safety procedures, refer to the Online Safety Frequently Asked Questions (FAQ) in Appendix 5. It covers the following topics on the relevant page as follows:

1 How will the policy be introduced to students? How will staff be consulted and made aware of this policy? How will complaints regarding Internet use be handled? How will parents' support be enlisted?
2 Why is the use of Internet and ICT important? How is the safe use of ICT and the Internet promoted? How does the Internet and use of ICT benefit education in our school? How will students learn to evaluate Internet content?
3 How is filtering managed? How are emerging technologies managed? How to react to misuse by students and young people
4 How is printing managed? What are the categories of Cyber-Bullying? What are the student rules?
5 What has research into Cyber Bullying found? What is the impact on a child of ICT-based sexual abuse? What is the impact on a child of ICT-based sexual abuse? How do I stay secure on the Internet? Why is promoting safe use of ICT important? What does the school's Mobile Phone Policy Include?
6 Where can we learn more about Prevent? What do we have to do?
7 Do we have to have a separate *Prevent* Policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?
8 What training must we have? What are the potential legal consequences if we do not take the *Prevent* duty seriously? What are the rules for publishing content online?

Related documents:

- Online Safety Appendices 1-6
- Safeguarding Children- Child Protection Policy; Sexual Violence and Sexual Harassment (Including Peer-on-Peer Abuse Policy); Anti-Bullying Policy; Behaviour and Discipline Policy; Staff Behaviour (Code of Conduct) Policy.
- Prevent Duty: Tackling Extremism and Radicalisation Policy; Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE); The School Rules.

- Mobile and Smart Technology Policy, including taking and storing images of students; Acceptable use of ICT Sign off forms for Staff/Students; Use of Photographs Sign-off Form.

Legal Status:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Students Safe in Education* (KCSIE) *Information for all schools and colleges* (DfE: currently in force) incorporates the additional statutory guidance,
- *Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.*
- *Working Together to Safeguard Students* (WT) (HM Govt.: Currently in force) which also refers to non-statutory advice, *Information sharing* HM Government: currently in force); *Prevent Duty Guidance: for England and Wales* (currently in force) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for schools and childminders (currently in force)* and *The use of social media for on-line radicalisation (currently in force) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE)*
- Based on guidance from the DfE (currently in force) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'
- Prepared with reference to DfE Guidance (currently in force) *Preventing and Tackling Bullying: Advice for school leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in schools.*
- Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*
- The Data Protection Act 1998; GDPR, 2018; BECTA and CEOP.
- Teaching Online Safety in School (DfE: currently in force)

Appendix 1 – Student and Parent/Carers acceptable use policy

The acceptable use policy below is expected to be read and signed by all students in Key Stage 3 and above and we ask parents to have read and understood the policy to support us with keeping children safe when using devices.

All students must follow the rules outlined in this policy when using school ICT resources and equipment, including all Internet access and the Virtual Learning Environment (VLE), accessed from both in and outside of school, and on school-provided or personal electronic devices. Breaking these conditions may lead to: confiscation of any electronic devices, close monitoring of the student's network activity, investigation of the student's past network activity, withdrawal of the student's access and, in some cases, permanent removal from the School and even criminal prosecution. Students are also expected to take care of school-issued electronic devices and any damage to them may result in charges to replace or fix damaged devices. Misuse of the Internet will be dealt with in accordance with the school's Behaviour and Discipline Policy and, where there is a safeguarding risk, the Safeguarding & Child Protection Policy. The school is not responsible for any loss of data on the network, computers connected to the network or data storage used on the network (including USB memory sticks). Data held on the network will be backed up for a limited period. Students are responsible for backups of any other data held. Use of any information obtained via the network is at the student's own risk.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school.

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:
- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Student agreement:

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:
- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, USB devices etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Print student name…… Class ……

Student Signature……..Date…….

Parent/Guardian agreement:

I understand that my child has agreed to accept the terms of the Online Safety and Student AUP Policy and I confirm that I accept the terms of the agreement. If my child brings any personal electronic devices to school, I understand that the student is responsible for its safekeeping and appropriate usage while in transit to and from and on campus.

I have read and understood the Online Safety policy and agree to check any updates, which are made available on the Parent Portal.

Print Parent/Guardian name…….

Parent/Guardian Signature…… Date…….

Appendix 2 – Staff and Volunteer Acceptable Use of ICT Policy:

To ensure that members of staff and volunteers are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this Acceptable Use Policy. Members of staff should consult the school's Online Safety policy and Staff Code of Conduct for further information and clarification. You must not use any ICT on-site until you have signed this AUP document and logged it with HR.

- I will respect all ICT equipment/facilities at Woldingham School and will report any faults I find or any damage I accidentally cause.
- I agree to abide by this policy in respect of any of my own ICT equipment or mobile devices that I bring on site. If any ICT device (personal or school-issued) is being used inappropriately or illegally on site (or inappropriately in the presence of students), the Head may request that the device be monitored. Failure to comply with the monitoring could result in informing the appropriate authorities.
- I understand that no photographs of students may be taken with or stored on my personal electronic devices, including cameras, iPads, mobile phones, or personal computers.
- Photos of students should not be uploaded to personal social media accounts
- I am familiar with the school's Data Protection Policy and I agree I am responsible for the security of all personal data in my possession. I agree that all personal data that relates to an identifiable person and is stored or carried by me on a removable memory device will be encrypted or contained within password-protected files to prevent unauthorised access.
- I am responsible for my use of my own log-in details and if I suspect that my log-in details have become known to others then I will immediately ask for these details to be changed.
- I agree that my use of Woldingham School ICT equipment/facilities will be monitored and may be recorded at all times. I understand that the results of such monitoring and recording may be shared with other parties if I break the terms of this Acceptable Use Policy.
- I will not deliberately attempt to access any unsuitable websites, services, files or other resources when on-site or using Woldingham School equipment/facilities. I understand that I may temporarily access-blocked websites, services and other online resources using only tools that are provided by Woldingham School. I agree that I will not display blocked websites, services and other resources to others until I have fully assessed the materials and have found them to be entirely suitable for the intended audience.
- I agree that the provision of Woldingham School ICT equipment/facilities including the email and Internet system are for educational purposes, although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other clauses in this document.
- I am aware that downloading copyright materials, including music and video files without paying the appropriate licence fee is often a criminal act. I am aware that any involvement in criminal acts relating to the use of ICT on-site or using Woldingham School equipment/facilities may result in disciplinary or legal action. I will not deliberately engage in these acts.
- I will not deliberately view, send, upload or download any material that is unsuitable for the school environment whilst I am in that environment or using any ICT equipment/facilities belonging to Woldingham School. If I accidentally encounter any such material then I will immediately close, but not delete in the case of emails, the material and immediately report it to the Online Safety Officer or to a senior member of staff. I will not be penalised if I view unsuitable material accidentally and by reporting such incidents I will help to improve Online Safety. If I am in any doubt about the suitability of any material, or if a colleague raises any doubts, then I will not (re)access the material without the agreement of the Online Safety Officer. I will not access any material that the Online Safety Officer has rated as unsuitable.
- Unless specifically authorised to do so, I will not disclose any of my personal details, other than those that identify me professionally, nor log any such details on websites whilst using Woldingham School equipment or facilities. If I disclose any additional personal details contrary to this instruction, then I agree that these details can be recorded and that I will not hold Woldingham School responsible for maintaining the security of the details I have disclosed.
- I agree that professional standards of communication will be maintained at all times. I recognise that staff should not communicate with students through personal electronic devices or methods such as social networking sites, blogging, chat rooms, text messaging, messenger applications or private email. Instead, only the school email system may be used.

Print Name _____ Signed _____ Date:_____

Appendix 3 - Mobile and Smart Technology Policy, including taking and storing images of students

Legal Status:
Teaching Online Safety in School: DfE (currently in force)
Cyberbullying: Advice of Headteachers and School Staff: DfE, (currently in force)
Department for Education's published guidance on the use of mobile phones and UK law governing the use of mobile phones while driving.

Applies to: This policy applies to all individuals who are to have access to and or be users of personal and/ or work-related mobile phones within the broadest context of the setting environment. This will include our students, parents and carers, volunteers, visitors, contractors and community users. This list is not to be considered exhaustive.

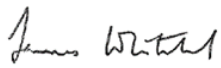
Related documents:
- Safeguarding & Child Protection Policy
- Behaviour Management Policy
- Anti-Bullying Policy

Availability:
This policy is made available to parents, staff and students in the following ways: via the School website, parent portal and on request, a copy may be obtained from the Office.

Monitoring and Review: This document will be subject to continuous monitoring, refinement and audit by the Head. This document was reviewed and agreed by the Board of Trustees in September 2022 and if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require, prior to September 2022, the policy will be reviewed accordingly.

Signed:

Reviewed: September 2022
Next Review: September 2023



Dr James Whitehead
Head

Mr Robert Parkinson
Chair of Governors

Introduction: Whilst we welcome the use of mobile phones and cameras for educational purposes and the convenience they offer and recognise that learning to use digital technology is an important part of the ICT and wider curriculum, equally we have to ensure the safeguarding needs of the students are met and staff, parents and volunteers are not distracted from their care of students. Mobile phones, alongside other technologies aim to change the way we communicate. This speed of communication will often provide security and reassurance; however, as with any other form of technology there are associated risks. Students and young people must be encouraged to understand such risks, to enable them to develop the appropriate strategies which will keep them safe. Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation that the personal use of mobile phones is to be limited to specific times and uses set out within the policy.

Aims: The aim of this Policy is to protect all users from harm, by ensuring the appropriate management and use of mobile phones by all individuals who work or visit our school, including students themselves. Students and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way; and to be alert to the potential risks of such use. This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

Policy statement: It is to be recognised that it is the enhanced functions of many mobile devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and cyberbullying. It must be understood that should mobile phones be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to students and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

Code of conduct: A code of conduct is to be promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the students and young people in their care. It is to be ensured that all teachers and staff will:

- Be aware of the need to protect students from harm.
- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Be vigilant and alert to potential warning signs of misuse.
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to potential allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Be responsible for the self-moderation of their own behaviours.
- Be aware of the importance of reporting concerns immediately.

Guidance on Use of Mobile Phones by Teaching Staff: The following points apply to all staff and volunteers at our school and apply to the use of all mobile devices to ensure the quality of supervision and care of the students, as well as the safeguarding of students, staff, parents and volunteers in the school.

Woldingham School allows staff to bring in mobile phones for their own personal use. However, they must be kept away in closed drawers or their bags when teaching, and are not allowed to be used in the presence of students. They may be used during working hours in a designated break away from the students. Staff are not permitted to use recording equipment on their personal devices to take photos or videos of students. If staff fail to follow this guidance, disciplinary action will be taken in accordance to Woldingham School Disciplinary Policy. During outings, nominated staff will be permitted to have access to their own mobile phones, which are to be used for emergency contact only. During off-campus activities, i.e. field trips and overnight excursions, trip leaders will be provided with a school-issued mobile phone in good working condition. School-issued mobile phones must be switched on and turned to loud to ensure that staff can be contacted by the school. Contact numbers for all members of staff accompanying the students must be left at Reception and a list of contact telephone numbers for all students should be with the leader of the off-site activity (although these must be kept confidential).

If staff need to make an emergency call, (such as summoning medical help or reporting an intruder on the premises) they must do so irrespective of where they are, via their own mobile phone or a school phone. Staff should provide the school number to members of the family and next of kin so in an emergency the member of staff can be contacted on the school phone. Staff must ensure that there is no inappropriate or illegal content on their phones or mobile devices. Should any member of staff become aware of inappropriate use of a mobile phone, this should be reported to a member of the SLT, and may be subject to disciplinary action.

All teachers are responsible for the storage of school mobile devices, which should be locked away securely when not in use. Images taken and stored on school devices should be uploaded to the school's secure network and deleted from the device when no longer required. Staff are not to use their own equipment to take photos of students. Under no circumstances must devices of any kind be taken into the student toilets (this includes any device with photographic or video capabilities).

Guidance on staff use of social media: Staff must not post anything onto social networking sites such as Facebook that could be construed to have any negative impact on the School's reputation. (We advise all our staff to carefully restrict their Facebook profiles to ensure they cannot be contacted by parents and students; this could involve removing their last name from their

page). We explain to staff that although they are able to accept friendship requests from friends, who may also be parents of students at the school, staff must be aware of the potential issues this could cause. Staff must not post anything onto social networking sites that would offend any other member of staff or parent. If any of the above points are found to have occurred, then the member of staff involved will face disciplinary action, which could result in dismissal. Where email contact is initiated by students who have left Woldingham School, employees may reply from a school email address only with blind copies to line managers **and** the DSL. Staff must not accept friendship requests from students on roll and we advise staff not to accept requests from former students.

Guidance on Use of Mobile Devices by Students (3G, 4G and 5G access): Dependent on age, some students are permitted to have mobile devices both in boarding houses and in academic school buildings. However, the school recognises that by using devices which have access to 3G, 4G and 5G mobile phone networks, this can result in children having unlimited and unrestricted access to the internet, which could lead to some children, whilst at school or college, sexually harassing their peers via their mobile and smart technology, sharing indecent images: consensually and non-consensually (often via large chat groups), and viewing and sharing pornography and other harmful content. The school takes precautions to ensure that students limit access to their personal mobile devices during the school day, and reserves the right to confiscate and monitor personal devices when deemed necessary for safeguarding concerns. During lessons, mobile devices should be switched off and kept securely in lockers, in their rooms or in their school bag unless permission has been given by the classroom teacher, such as for use in note taking or data collection. In the event of a mobile phone being used in a lesson without permission from the teacher, the phone should be confiscated and given to the Head.

Woldingham School values the health and wellbeing of every student. To this end, boarding students MUST not use their mobile phones or mobile devices after evening checks are made in the Houses or after evening "lights out" unless specific arrangements have been made to contact family in a different time zone.

In the boarding houses, mobile phones are permitted during free time, although their use is prohibited after lights out. Phones can be collected from younger students (up to Year 10) and this provision can be extended to students who persistently use their phones at inappropriate times. Mobile devices must not be used to directly take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission. Students and staff are informed about the statutory framework regarding the sharing and publishing of photographs and videos, regardless of the media chosen. Staff must adhere to the Safeguarding & Child Protection Policy and Staff Code of Conduct. Woldingham School acknowledge that due to the international nature of the School and the student body that it is acceptable for some students to contact family members, after lights out, where time zones do not align with GMT or BST.

The School has the right to confiscate and search any mobile electronic device (personal or school-issued) if it suspects that a student or staff member is in danger or has misused a device. This will be done in accordance with the School's policy on searching and confiscation as set out in the Behaviour and Discipline Policy.

Unacceptable Uses: In order to protect one's privacy and respect to others, unless express permission is granted, mobile phones, laptops and mobile devices should not be used to make calls, send messages, use the internet, take photos or use any other application during school lessons, other educational activities such as assemblies, or in the Woldingham School Dining Halls.

- Mobile devices should not disrupt classroom lessons with ring tones, music or beeping. They should be turned off during lesson times in order to respect the learning environment.
- Using mobile devices to intimidate, bully, harass, threaten, attempt to radicalise others or breach copyright laws is unacceptable. Cyber bullying will not be tolerated. In some cases, it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. (Please refer to our Anti-bullying Policy)
- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.
- Disruption to lessons caused by a mobile phone or any mobile device may lead to disciplinary consequences.
- Any student who uses vulgar, derogatory, or obscene language while using a mobile phone may face disciplinary action.
- Safeguarding, privacy and respect are paramount at Woldingham School. To this end, it is prohibited to take a picture of

or record a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images and may be requested to turn over the device to the Head and/or the Designated Safeguarding Lead.

- For safety reasons, headphones/earphones should not be used whilst moving around campus during the school day, whilst waiting for or during lessons and assemblies, or in the Woldingham School dining halls
- Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

This may result in disconnection from the school network, confiscation of the mobile technology and/or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission and if in doing so, School and statutory guidelines are not breached.

Theft or damage: Mobile phones or any mobile devices that are found in the school and whose owner cannot be located should be handed to the front office reception. The school accepts no responsibility for replacing lost, stolen or damaged devices. The school accepts no responsibility for damage to or loss of mobile phones or mobile devices while travelling to and from school. **It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones or other mobile devices. Students must keep their password/pin numbers confidential.**

Inappropriate conduct: Under exam regulations, mobile phones are prohibited from all examinations. Students MUST give phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.

Use of images: displays etc

We will only use images of our students for the following purposes:

- Internal displays (including clips of moving images and yearbooks) on digital and conventional notice boards within School premises.
- Communications with Woldingham School community (parents, students, staff), for example newsletters and E-learning Journals.
- Marketing Woldingham School, both digitally by website, by prospectus [which includes a DVD and YouTube channel], by displays at educational fairs and other marketing functions [both inside the UK and overseas] and by other means.

Storage and Review of Images: Images of students should be stored securely on the school network. Digital photographs and videos are reviewed annually and are deleted when no longer required. We regularly check and update our web site, with expired material deleted.

Woldingham School Website and Social Media Pages: Photographs and videos may only be uploaded to the school's website or social media accounts with the Head's approval. Student's surnames are never used on our website or social media pages.

Images that we use in displays and on our web site: The images that we use for displays and communications purposes never identify an individual student. Instead, they name the event, the term and year that the photograph was taken (for example, 'Sports Day, Summer Term 2021'). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc. in their proper context. We never use any image that might embarrass or humiliate a student. Students are always properly supervised when professional photographers visit Woldingham School. Parents are given the opportunity to purchase copies of these photographs.

External Photographers: Professional photographs are taken throughout the year at school shows, by local media and Professional School Portraits. The Head ensures that professional photographers are DBS checked and that they have their own stringent regulations, which ensure safeguarding of students from inappropriate use of images.

Media coverage: We will always aim to notify parents in advance when we expect the press to attend an event in which our students are participating, and will make every effort to ensure that images including students whose parents or guardians have refused permission for such images of their students to be used are not used. We will always complain to the Independent Press Standards Organisation (IPSO) if the media fails to follow the appropriate code of practice for the protection of young people, including the students of celebrities.

Staff induction: All new teaching and office staff are given guidance on the school's policy on taking, using and storing images of students.

Parents/Visitors and Volunteers use of mobile phones/cameras within the school buildings (Including Photographing Pupils: Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of students or in public areas of the school such as during meetings and school events. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in and around the school. The exception to this would be at an organised event. Staff should remind parents regularly of school policy with regard to mobile phone use with the following statement on weekly emails, when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g. a family album) and so are exempt from data protection Laws. Please be aware these images (which may include other students) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of data protection." If they wish to make or take an emergency call, they may use the office and the school phone.

The school records images of students, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of students while performing and disturbance within the audience.

Parents are welcome to take photographs of their own students taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events. Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts. We always print a reminder in the programme of events where issues of copyright apply. Additionally, the school records images of students, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph professionally events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of students while performing and disturbance within the audience.

When students join Woldingham School, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld, this must be made clear when the consent form is returned to school so that photographs/videos are not published of the individual child concerned. The students take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents are welcome to take photographs of these memorable events, which may include groups of students. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents. Wherever possible, parents who take photographs of groups of children who are in the care of the school should gain consent first, ensuring that once any photographs are taken, they are stored safely and not posted to social media. The school recognises that it cannot police parents taking photographs of pupils who are outside school grounds and not in the school's care, however posting such pictures online may be in breach of data protection laws without consent of all people within the photograph.

Other mobile technology: At Woldingham School, we recognise the value of mobile technology within our curriculum and our students' accommodation. Within the upper school, students are required to bring their own devices to support their studies. Any personal device that students bring to the school must be used appropriately in line with the Students' Acceptable Use Policy and must be kept securely. Where a student is found to be misusing a school or personal device, or accessing inappropriate content, the device may be confiscated by the school and appropriate action taken. When accessing the school

WiFi, staff and students must adhere to their ICT Acceptable Use Policy. Staff, students, volunteers and parents are responsible for their own mobile devices and the school is not responsible for theft, loss, or damage.

Driving and the law: The use of hand-held phones while driving, whether to make or receive a call, is prohibited. The only exception to this will be in the event of a genuine emergency call to 999 or 112, if it would be unsafe for the driver to stop. Hand-held mobile phones used with an earphone and microphone are covered under the ban, as they still require the user to hold the phone to press buttons or to read a message on the phone's screen. Mobile phones must instead be directed to the message/voicemail service while driving. The Head will not assist in the payment of any fine levied against anyone using a hand-held mobile phone while driving. An employee will be regarded as driving if the engine is running, even if the vehicle is stationery. Notification of any contravention of these requirements may be regarded as a disciplinary matter.

Appendix 4 – Use of photographs of students and data protection form (to be completed by all new parents)

Photographs

Woldingham School would like your permission to use photographs of your child for marketing and publicity purposes including our website, prospectus, adverts, press releases and other marketing literature such as brochures and leaflets. We will not use names next to photographs of students on the website (in accordance with the DfE guidelines).

Parent/Guardian's name: _____

Pupil's name: _____

Pupil's year group/form: _____

Please tick the appropriate box.

I give my permission for Woldingham School to use photographs of my child for marketing and publicity purposes ☐

I do not give my permission for Woldingham School to use photographs of my child for marketing and publicity purposes ☐

Signature: _____ Date: _____

Data Protection Statement

Information about parents/carers is collated, stored and used by Woldingham School for the purposes of keeping you informed of events and activities concerning Woldingham School and for fundraising. By signing this form, you consent to Woldingham School using your data in this way. This information will not be used for any other purpose or passed to any person outside the school without your consent.

I consent to Woldingham School using my data for the stated purposes ☐

I do not consent to Woldingham School using my data for the stated purposes ☐

Signature: _____ Date: _____

Appendix 5: Online Safety FAQs

How will the policy be introduced to Students?

- Rules for Internet access will be posted in all rooms where computers are used
- Students will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access
- A module on responsible Internet use will be included in the PSHE programme covering both home and school use.
- Students will be informed that network and Internet use will be monitored and appropriately followed up.
- Students will be made aware of the acceptable use of technology and sign upon enrolment

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security
- Security strategies will be discussed at staff meetings.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as USB sticks, SD Cards and Hard Drives to carry work should be kept confidential by staff and not used in public computers.
- Files held on the school network will be regularly checked
- All network system and administration passwords are to be recorded by the IT Department and kept in a secure place with regular updates

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the 'Responsible Internet Use' statement included in the staff handbook before using any Internet resource in school.
- All new staff will be taken through the key parts of this policy as part of their induction.
- All staff including teachers, learning support assistants and support staff will be provided with the School Online Safety policy and have its importance explained as part of the child protection training requirement.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.
- Breaching this Online Safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
- Staff will read the ICT Acceptable Use Policy and sign the form prior to using school ICT equipment in the school

How will complaints regarding Internet use be handled?

- Responsibility for handling complaints that have progressed to Stage 2 will be delegated to a relevant member of the Senior Leadership Team.
- Complaints of Internet misuse will be dealt with by the Head.
- Any complaint about staff misuse must be referred to the Head.
- Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy and procedures.
- Students and parents will be informed of the complaint procedure which is available on the Woldingham School website.
- Parents and Students will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the responsible Internet use policy in newsletters, the parent portal and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach will be encouraged with parents and could include information booklets, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

- We will maintain a list of Online Safety resources for parents.
- Parents will be invited to attend an Online Safety workshop annually.

Why is the use of Internet and ICT important?

Not only is familiarity with the use of ICT equipment a core requirement, but the efficient use of the equipment and available resources is also considered key – for example, the use of email for efficient communication and the correct use of the Internet for research. Staff across the school are making increased use of ICT, which benefits not only the quality of teaching and support services but also their professional development. It is equally important that staff are properly equipped and supported to make the most efficient use of ICT resources. In particular, ICT is extremely beneficial in engaging our students, who have learning and physical disabilities. It can also help them to access parts of the curriculum, which they might not otherwise be able to engage with.

All students deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" ICT facilities including online resources and services. Internet use is a part of the statutory curriculum and a necessary tool for staff and Students. The school has a duty to provide Students with quality Internet access as part of their learning experience. In order for the school to maintain such an environment for learners (students and adults) everybody must be aware of the need to ensure online protection (Online Safety) and subsequently understand the principles of this policy and the expectations of school practice as documented below.

How is the Safe Use of ICT and the Internet Promoted?

Woldingham School takes very seriously the importance of teaching students (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community. Woldingham School has in place an Internet firewall, Internet content filtering and antivirus software, and various IT security policies, which help to ameliorate the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe and Woldingham School will further promote safe use of ICT and the Internet by educating students and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly. The school will ensure that the use of Internet derived materials by staff and Students complies with copyright law. Woldingham School will help students to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially students, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our PSHEE and SMSC provision. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- PSHE Association (https://www.pshe-association.org.uk/)
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

How does the Internet and use of ICT benefit education in our school?

- Students learn effective ways to use ICT and the Internet including safe and responsible use.
- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between Students worldwide.
- Access to experts in many fields for students and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with LA and DfE
- Support of the wider curriculum through the use of word processing, spreadsheet and presentation tools, specialist applications, and the use of the Internet for research purposes.

How will Students learn to evaluate Internet content?

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.
- Students will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.

- If staff or Students discover unsuitable sites, the URL (address) and content must be reported to the teacher, Online Safety Officer or IT Department.
- Staff and Students should ensure that their use of Internet derived materials complies with copyright law
- Students will be taught the SIFT Model to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright.

How is Filtering Managed?

Having Internet access enables students to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. All unsuitable websites will be filtered and automatically blocked by our security systems and will not be made accessible to students. In addition, students' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert our IT Department. The IT Department will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of students. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some students may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at Woldingham School we believe that the benefits to students having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of minors along with Woldingham School share the responsibility for setting and conveying the standards that students should follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide students towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio.

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, they must report it to the DSL or Chair of Governors immediately.
- The school will take every step to ensure that appropriate filtering systems are in place to protect students from unsuitable material and the methods used will be reviewed regularly.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk).

How are Emerging Technologies Managed?

ICT in the 21st Century has an all-encompassing role within the lives of students and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by students may include:

- The Internet
- E-mail
- Instant messaging / video messaging apps (WhatsApp / WeChat / iMessage)
- Social media sites (Facebook, Instagram, Twitter, TikTok)
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (Popular: http://www.youtube.com/ ,Twitch)
- Chat Rooms (Popular www.teenchat.com, Discord)
- Gaming Sites
- Music download sites (Popular Apple, Spotify,)
- Smart Phones (where all of the above can be accessed)
- Mobile technology (e.g. games consoles)

How to React to Misuse by Students and Young People

• **Step 1:** Should it be considered that a child or young person has deliberately misused ICT, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.

• **Step 2:** If there are to be further incidents of misuse, the child or young person will be suspended from using the Internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with a member of the Leadership Team and the most appropriate course of action will be agreed.

• **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding & Child Protection Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

How is Printing Managed?
The use of the ICT printers may be monitored on an individual basis to encourage careful use of printing resources. As well as being a significant capital cost, the consumables (ink, laser printer toner and drums, and paper) associated with printing represent one of the most expensive ongoing costs associated with ICT. Whilst the school would not wish to discourage the proper use of printers, it is important to ensure that printing facilities are used efficiently and effectively. Students and staff are asked to take care not to waste printing resources, for example by using "Print Preview" to check work before sending it to the printer and by using colour print only when necessary.

What are the categories of Cyber-Bullying? Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to students or young people, or posting inappropriate material in a public digital locale.
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where students and young people are sent unpleasant messages as they conduct real-time conversations online.
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

General Housekeeping:
The ICT equipment used by the school represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order. In addition, the ICT resource is finite e.g. computers can run out of disk space; users should be encouraged to think about the amount of file storage they use and the need to keep it well organised. The school does not currently operate a quota system for disk space or mailboxes, but will consider doing so should the need arise.
The following will apply:

- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy.
- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

Student Rules when using school ICT: Due to the variety of resources throughout the school, including the use of portable digital equipment, the following rules are to be considered as appropriate to the location and the resource.

- Obtain permission to access school-issued ICT resources.
- Food and drink must not be consumed near any computer equipment anywhere in the school.
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.
- Computer/device faults should be promptly reported to the ICT Co-ordinator. Please do not attempt to repair them yourself.

- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at a workstation when possible.
- At the end of a session using an computer station:
- Log off/shut down according to instructions.
- Replace laptops/equipment as directed.
- Wind up and put away any headsets.

What has Research into Cyber Bullying Found?

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyber-bullying is done by students in the same class or year group and although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

- Between a fifth and a quarter of students have been cyber-bullied at least once over the previous few months.
- Phone calls, text messages and email are the most common forms of cyber-bullying.
- There is more cyber-bullying outside school than in.
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone.
- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying.
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying.
- Website and text bullying are equated in impact to other forms of bullying.
- Around a third of those being cyber-bullied tell no one about the bullying.

What is the impact on a child of ICT based sexual abuse?

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

Why is Promoting Safe Use of ICT Important?

Woldingham School takes very seriously the importance of teaching students (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community.

What does the school's Mobile Phone Policy Include?

- The commitment to keep the students safe.
- How we manage the use of mobile phones at Woldingham School taking into consideration staff, students on placement, volunteers, other professionals, Board of Governors, visitors and parents/carers.
- How we inform parents/carers, visitors and other professional of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

What are the rules for publishing content online?

- Staff or Student personal contact information will not be published on the school website. The only contact details given on our website will be the school address and telephone number.
- Student's full names will not be used anywhere on the school website or other on-line space.
- We may use photographs of students or their work when communicating with parents and the wider community, in newsletters and in the school prospectus.
- Photographs will be checked to ensure that they are suitable (photos of students in swimwear would be unsuitable).

Appendix 6 - Acceptable Use of Mobile Phones and 3G/4G/5G compatible devices

It is our intention to provide within this policy an environment in which children, parents, and staff are safe from images being recorded and inappropriately used, in turn eliminating the potential use to interfere with the dignity and privacy of all individuals and thus compromise the confidentiality of the children in our care.

Purpose:

- The widespread ownership of Mobile phones and 3G/4G/5G compatible devices (referred to throughout this document as mobile devices) among young people requires that school administrators, teachers, students, parents and carers take steps to ensure that these devices are used safely and responsibly at school. This Acceptable Use Policy is designed to ensure that potential issues involving mobile devices can be clearly identified and addressed, ensuring the benefits that they can provide can continue to be enjoyed by our students.
- The school has established the following Acceptable Use Policy for mobile devices that provides teachers, students, parents and carers guidelines and instructions for the appropriate use of these devices during the time students are under the care of the school, inclusive of the academic day, the boarding program, on campus and all educational visits.
- Students, their parents or carers must read and understand the Acceptable Use Policy as a condition upon which permission is given to bring mobile devices to school.

Rationale:

- The school recognises that personal communication through mobile devices such as mobile technologies is an accepted part of everyday life, therefore such technologies are to be used responsibly and in accordance to the Acceptable Use Policy.
- Woldingham School accepts that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact their child if they need to speak to them urgently.

Responsibility:

- It is the responsibility of students who bring mobile devices to school to follow the guidelines outlined in this document. The decision to provide any mobile devices to their children should be made by parents or carers. It is important that parents understand the capabilities of these devices and the potential uses or misuses of those capabilities. If needed, guidance to this information can be signposted by the school.
- Parents/carers should be aware that if their child brings any device, including a mobile phone to school, the school does not accept responsibility for any loss, damage or costs.
- Parents/carers are reminded that in cases of emergency, the school remains a vital and appropriate point of contact and can ensure your child is reached in a relevant and appropriate way. Parents/carers are requested that in cases of emergency they contact the school first so we are aware of any potential issue and may make any necessary arrangements.

Acceptable Uses:

- Mobile phones should be switched off and kept out of sight during classroom lessons in order to minimise disruption or distraction.
- Mobile phones should not be used in any manner or place that could be disruptive to the normal routine of the school.
- The school recognizes the importance of emerging technologies present in modern mobile devices e.g. phones, camera and video recording, internet access, MP3 and MP4 playback, blogging, etc. Teachers may wish to utilise these functions to aid teaching and learning and students may have the opportunity to use their mobile phones or mobile devices in the classroom. On these occasions students may use their mobile phones in the classroom when express permission has been given by the teacher. The use of personal mobile phones in one lesson for a specific purpose does not mean blanket usage is then acceptable.
- Headphones/earphones should only be used during private study or travelling to and from school with permission from the teacher.

Unacceptable Uses:

- In order to protect one's privacy and respect to others, unless express permission is granted, mobile phones, laptops and mobile devices should not be used to make calls, send messages, surf the internet, take photos or use any other application during school lessons, other educational activities such as assemblies, or in the Dining Hall.
- Mobile devices should not disrupt classroom lessons with ring tones, music or beeping. They should be turned off during lesson times in order to respect the learning environment. Using mobile phones to bully and threaten other students is unacceptable. Cyber bullying will not be tolerated. In some cases, it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. (Please refer to the Anti-bullying and Online Safety Policies.)

- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.
- Disruption to lessons caused by a mobile phone or any mobile device may lead to disciplinary consequences.
- Safeguarding, privacy and respect are paramount at Woldingham School. To this end, it is prohibited to take a picture of or record a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images and may be requested to turn over the device to the Head and/or the Designated Safeguarding Lead.
- Headphones/earphones should not be used whilst moving around campus during the school day, whilst waiting for or during lessons and assemblies, or in the dining halls.

Theft or damage:
- Mobile phones or any mobile devices that are found in the school and whose owner cannot be located should be handed to the front office reception.
- The school accepts no responsibility for replacing lost, stolen or damaged devices.
- The school accepts no responsibility for damage to or loss of mobile phones or mobile devices while travelling to and from school.
- It is strongly advised that students use passwords/pin numbers to ensure that unauthorized phone calls cannot be made on their phones or other mobile devices. Students must keep their password/pin numbers confidential.

Inappropriate conduct:
- Under exam regulations, mobile phones are prohibited from all examinations. Students MUST give phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.
- Any student who uses vulgar, derogatory, or obscene language while using a mobile phone may face disciplinary action.
- In order to ensure all boarders study time is respected, boarding students MUST not use their mobile phones or mobile devices during evening study hall hours unless explicitly required by their teacher for a specific assignment.
- The school values the health and wellbeing of every student. To this end, boarding students MUST not use their mobile phones or mobile devices after evening checks are made in the Houses or after evening "lights out".
- Students with mobile phones may not engage in personal attacks, harass another person, or post private information about another person using messages, taking/sending photos or objectionable images, and phone calls. Students using mobile phones to bully other students will face disciplinary action. (It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, the school may consider it appropriate to involve the police).
- Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence, and the school is obliged to report any findings of this nature to the police and local authority.
- Similarly, 'sexting' – which is the sending of personal sexual imagery - is also a criminal offence, which obliges the school to report to the police and local authority.

Measures: The following measures may be used in consultation and conjunction with the Anti-bullying , Child Protection and Safeguarding, Online Safety and IT Policies. The Online Safety Coordinator (DSL) must be consulted when inappropriate conduct requires a mobile phone to be confiscated and searched.
- Students who violate the rules set out in this document could face having their phones and/or mobile devices held by teachers, House Parents, Deputy House Parents or House Tutors until the end of the class period or study session. If the device is being used inappropriately the student must give it to the supervising adult if requested.
- Violation of the rules set out in this document are subject to the disciplinary measures set out in the Behaviour Management Policy, which can be found on the policy section of the school's Website.

I have read and understand this policy:

Student signature: _____ Parents: Informed via email communication


Student Acceptable Use Policy (AUP)
E
Ensure that I do not create, send or post anything which is offensive to other people or brings the school into disrepute. I will not use any language or images which could offend any minority group.
S
Secure all my passwords and not share them with others. I understand I must not reveal or use anyone else's login details or access a device someone else is logged onto. I will change my password immediately if it becomes known to someone else and ensure I log out after every network session.
A
Access only appropriate material. I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that school can monitor my use of the internet if any poor conduct is suspected. I will report any accidental access to other people's information, unsuitable websites or receipt of any inappropriate material as well as any security risk or suspicious behaviour that I become aware of. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity.
F
Facebook, social media and email use. I will not publish my own and others' personal details, information or location over any social networking site. I am aware that email is not guaranteed to be private. Messages or any communication via social media or email supporting illegal activities will be reported to the authorities.
E
Exercise caution when downloading material. I understand that the illegal download and/or copyright of any material, including receiving, sending or publishing, is forbidden and may be passed to the relevant authorities. I will not download any unapproved software, system utilities or resources from the internet.
T
Turn off mobile hot spots and not use the network in any way that will disrupt its use for other people. This includes any attempt to harm, destroy or remove any equipment, work of another user, or website connected to the system.
Y
Your device, your responsibility. I understand that the school has the right to confiscate and search any device if it suspects that a student is in danger or has misused a device or the school network. I understand that any activity from a device I own is my responsibility, including all portable devices and their content or viruses.