WINDLESHAM HOUSE SCHOOL

ONLINE SAFETY POLICY

Approved: **20 June 2022**
Last Technical Review: **Sep 2022**
Next Review date: **June 2023**

Policy Ref 01-02

Responsible Staff: **Christopher Roche**
Responsible Governor: **David Armitage**

Summary Policy Statement: At Windlesham, ICT is an integral part of day to day life and has an impact on every child and staff member. We aim for our children to be responsible and effective users of technology and they are provided with opportunities to use ICT in their academic and extra-curricular life at School. We have robust systems in place to keep our children safe whilst using technology as a teaching and learning tool, beyond this, all members of the School Community are educated in avoiding the potential dangers associated with online lives outside of the School.

This policy and procedures also apply to our Early Years Foundation Stage and after School care.

1. Policy Statement

1.1 Windlesham House School recognises that ICT and the Internet are integral tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to collaborate and share ideas can benefit all members of the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that pupils, staff and parents use it responsibly, appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

1.2 Online safety covers the Internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

1.3 There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school

community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

1.4 Cyber-bullying by pupils (both in and out of school) will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. (See Anti-bullying policy)

2. Roles and Responsibilities

2.1 Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. Online safety also falls within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include:

- ensure an online safety policy is in place, reviewed every year and is available to all stakeholders;
- ensure that there is an online safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive;
- ensure that procedures for the safe use of ICT and the Internet are in place and adhered to; and
- hold the headteacher and staff accountable for online safety.

2.2 Headteacher and SLT

The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety co-ordinator. Any complaint about staff misuse must be referred to the online safety coordinator at the school or, in the case of a serious complaint, to the Headmaster, to ensure:

- access to induction and training in online safety practices for all users.
- appropriate action is taken in all cases of misuse.
- Internet filtering methods are appropriate, effective and reasonable.
- staff or external providers who operate monitoring procedures be supervised by a named member of SLT.
- pupil or staff personal data as recorded within school management system sent over the Internet is secured;
- the School works in partnership with the DFE and the Internet Service Provider and school ICT Manager to ensure systems to protect pupils are reviewed and improved;
- the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly; and
- the Senior Leadership Team will receive monitoring reports from the online safety co-ordinator.

2.3 Online safety coordinator (The School Technology Provider, CTS):

- Leads E-safety meetings.

- Work in partnership with the DFE and school Network Manager to ensure systems to protect pupils are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments,
- Reports to Senior Leadership Team.
- Liaise with the nominated member of the governing body & headteacher to provide an annual report on online safety.

2.4 Network Manager / Technical Staff:

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply;
- That users may only access the networks and devices through a properly enforced password protection policy;
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person;
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher; online safety coordinator for investigation / action / sanction;
- That monitoring software / systems are implemented and updated as agreed in school policies; and
- Provide reports to governors on the above.

3. Communicating School Policy

This policy is available for staff online on the SharePoint at Staff/Bursary/2022-2023 Policies or by request pupils and parents. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

4. Making use of ICT and the Internet in school

4.1 The Internet is used in school to raise educational standards, aware of the online/digital environment to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary ICT skills that they will need in order to enable them to progress confidently and safely into a professional working

environment when they leave school. Some of the benefits of using ICT and the Internet in schools are:

4.2 For pupils:

- Access to worldwide educational resources and institutions such as art galleries, museums and libraries;
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world;
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen;
- Access to learning whenever and wherever convenient;
- Freedom to be creative;
- Freedom to explore the world and its cultures from within a classroom;
- Social inclusion, in class and online;
- Access to case studies, videos and interactive media to enhance understanding; and
- Individualised access to learning.

4.3 For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to pupils and parents.
- Class management, attendance records, schedule, and assignment tracking.

4.4 For parents:

Communication between School and Home on issues related to the education of their children and issues faced by the challenges and potential dangers of the online world.

The main forms of communication are via Email, Parent Whatsapp groups or text messaging.

5. Learning to Evaluate Internet Content

5.1 With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Pupils will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate;
- Use age-appropriate tools to search for information online; and

- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Pupils who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

5.2 The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils.

5.3 If a member of staff or pupils discover unsuitable sites then the URL will be reported to the school online safety coordinator.

5.4 Any material found by members of the school community that is believed to be unlawful will be reported to the online safety coordinator.

5.5 Regular software and broadband checks will take place to ensure that filtering services are working effectively.

6. Managing Information Systems

6.1 Windlesham House is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The Network Manager will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted and in accordance with our Data Protection Policy;
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this;
- Files held on the school network will be regularly checked for viruses;
- The use of user logins and passwords to access the school network will be enforced;
- Multi Factor Authentication is enforced on all staff accounts
- Staff receive regular training on Cyber Security issues
- Net work Manager runs regular mock attack simulations and appropriate training is provided to staff who fail the attack.
- Portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team;
- Compliant with existing Data Protection legislative requirements;
- LightSpeed filters all internet traffic and blocks sites which are deemed to be inappropriate. Internet searches are filtered for profanities, spam and any inappropriate content;
- Impero Software Actively monitors website titles, content, open applications and typed words for safeguarding, security and behavioural misuse of the computers – taking screenshots and (optionally) blocking access as Network Manager sees fit; and

- Virus protection throughout the school is updated daily.

6.2 For more information on data protection in school please refer to our Data Protection Policy found on the SharePoint at Staff/Bursary/2022-2023 Policies.

7. Emails

7.1 The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

7.2 Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, pupils, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to. See Staff Behaviours Policy and Staff Handbook.

8. School Email Accounts and Appropriate Use

8.1 All Prep School children have their own Exchange/Webmail account. Children have no access to any other email accounts in school. Pupil email addresses are constructed using the first four letter of their first name and the first four letters of their surname.

8.2 Children do not have access to external web-based email accounts such as Hotmail, Google mail etc.

8.3 Pupils must complete, sign and understand the Technology Rules of the Road Acceptance Agreement before using the School's ICT.

8.4 Staff have an Exchange email account which is accessible via the school network, remote access or via Smartphone (iPhone or Android). Staff are allowed to access their own personal emails via the school network.

8.5 Staff must authenticate their accounts using multi factor authentication before accessing their school email.

8.6 Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers for school related matters. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

8.7 Pupils should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In school, pupils should only use school-approved email accounts;
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves; and
- Pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

8.8 Pupils will be educated through the Computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

9. Published Content and the School Website

9.1 Windlesham House website is viewed as a tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, pupils, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

9.2 The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published (unless with express consent), and details for contacting the school will be for the school office only. For information on the school policy on use of children's photographs on the school website please refer to our Data Protection Policy.

9.3 As a marketing and information tool, the school website is maintained by the Marketing team and third party website specialists as they see fit.

10. Policy and Guidance of Safe Use of Children's Photographs, Film and Work

10.1 Photographs, film and pupils work bring Windlesham to life, showcase Windlesham pupil's talents, and add interest to publications both online and in print that represent Windlesham. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

10.2 On admission to the school parents/carers will be asked to sign an image consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of images and film of children, including:

- How and when the photographs and film will be used;
- How long parents are consenting the use of the images for; and
- Refer to our privacy policy and Data Protection Policy.

10.3 A template of the consent form can be found at Annex C.

10.4 Photographs, film or any other types of image of pupils must not be uploaded onto personal social media unless the pupil's family consent has been given. For example, if your child is friends with a pupil who appears in a picture alongside them, the parents' permission must be sought before uploading of pictures of the children on to social media.

10.5 Windlesham's digital camera/s or memory cards must not leave the school premises except for use on outings. Photos are printed in the setting by staff and images are then removed from the camera's memory.

11. Using photographs of individual children

11.1 The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

11.2 It is important that published images do not identify pupils or put them at risk of being identified. The school is careful to make sure that images published on the school website are difficult to reuse or manipulate through browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the parent's and school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications
  - on the school website
  - in newspapers as allowed by the school
  - in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a pupil in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child, unless express parental consent have been obtained. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of pupils such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.

11.3 For more information on safeguarding in school please refer to our school Child Protection and Safeguarding Children Policy.

12. Complaints of Misuse of Photographs or Video

12.1 Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our Complaints Policy and Procedure for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools Child Protection and Safeguarding Children Policy.

12.2 Cyberbullying and sexting by pupils will be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm and will be managed through our anti-bullying procedures (See our Anti-Bullying Policy) and Child Protection and Safeguarding Children Policy. Serious incidents may be managed in line with our Child Protection and Safeguarding Children Policy.

13. Training

13.1 Pupils

Many pupils own or have access to handheld devices and parents are encouraged to consider measures to keep their children safe when using the internet and social media at home and in the community.

Prior to using ICT at Windlesham House School, pupils must complete a 'Rules of the Road' (User Agreement), which outlines the rules of using ICT at the School. This can be found in Annex B.

13.2 Parents

The School regularly provides parent workshops (TechMeetUps) to make parents aware of how their children can use ICT in a safe manner. In addition, sessions focus on strategies to extend this safeguarding beyond the School and into the family home.

13.3 Teaching Staff

All teaching staff receive online safety training on an annual basis. In addition, INSET sessions related to the latest online safety trends are held at different times of the year.

13.4 Governors

All Governors receive online safety training on an annual basis.

14. Social Networking, Social Media and Personal Publishing

14.1 Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take

responsibility for their conduct online. Pupils are not allowed to access social media sites in school as the majority of our pupils do not meet the minimum required age. There are various restrictions on the use of these sites in school that apply to staff.

14.2 All network users must use an appropriate password and always remember to log out after use. It is the responsibility of the user and it is critical that staff do not allow children access to their own personal account.

14.3 This policy deals with Social media sites have many benefits for both personal use and professional learning; however, both staff and pupils should be aware of how they present themselves online. Pupils are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

14.4 Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways when they meet the required minimum age limit. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.

14.5 Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

14.6 Official school blogs created by staff will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.

14.7 Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.

14.8 Safe and professional behaviour of staff online will be discussed at staff induction.

15. Staff use of Social Media

15.1 Staff should be professional, responsible and respectful when using social media.

15.2 When using social media staff must be conscious at all times of the need to keep your personal and professional lives separate. Staff should not put themselves in a position where there is a conflict between their work for the School and their personal interests.

15.3 Staff must not:

- engage in activities involving social media which could damage the reputation of the School, even indirectly.
- represent their personal views as those of the School on any social media. Staff should write in the first person and use a personal email address.
- discuss personal information about School pupils, staff members and other professionals they interact with as part of their job at the School on social media.

- include the School's logos or other trademarks in any social media posting or in their profile on any social media.
- use social media and the Internet in any way to harass, bully, unlawfully discriminate against, attack, insult, abuse, disparage or defame pupils, their family members, staff members, other professionals, other organisations or the School as an institution; to make false or misleading statements; or to impersonate colleagues or third parties.
- express opinions on behalf of the School via social media, unless expressly authorised to do so by the Marketing Department. Staff may be required to undergo training in order to get such authorisation
- edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the School.
- identify themselves as employees of the School or service providers for the School in their personal web space (use of professional web space such as LinkedIn is up to the user's discretion, keeping in mind that anyone such as parents, pupils and colleagues can access your profile and you must always comply with this policy). This is to prevent information on these sites being linked with the School and to safeguard the privacy of staff members, particularly those involved in providing sensitive front-line services.
- accept 'friend requests' from current pupils or recent leavers they receive in their personal social media accounts.
- "check in" or tag their photos/videos at the School (this includes but is not limited to Facebook, Instagram, Twitter, Pinterest).
- use School email addresses and other official contact details for setting up personal social media accounts or to communicate through such media. The use of School email addresses to create or join a School sanctioned social media site is appropriate.
- on leaving the service of the School, contact the School's current pupils by means of personal social media sites. Similarly, staff members must not contact current pupils from their former schools by means of personal social media unless they are family-related/close friends with parents. It is advised to maintain professional conduct while communicating with former pupils for work or personal reasons.
- have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- have contact through any personal social media with any current pupils, whether from the School or any other school, unless it is for professional contact or the pupils are family members.

15.4 Staff must be:

- respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the Internet for anyone to see.
- accurate, fair and transparent when creating or altering online sources of information on behalf of the School.

15.5 If staff are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your Department Head.

15.6 If staff see social media content that disparages or reflects poorly on the School, they should contact a member of Senior Leadership Team (SLT).

15.7 The School permits limited personal use of social media while at work. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the Internet or social media should not be used during contact time (for teachers and teacher assistants), should never involve unprofessional or inappropriate content and must always comply with this policy.

15.8 Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Be mindful of having colleagues as friends on social media as it may be difficult to maintain professional relationships or it might be just embarrassing if too much personal information is known in the workplace.

15.9 Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and opt out of public listings on social networking sites to protect their own privacy.

15.10 Staff members can only use officially sanctioned School social media tools for communication on behalf of the School. Requests for this type of communication should go via the Marketing Department who have access to the relevant social media tools.

15.11 There must be a strong pedagogical or business reason for creating official School social network sites to communicate with pupils or others. Staff members must not create sites for trivial reasons which could expose the School to unwelcome publicity or the posting of unwelcome material or damage its reputation.

15.12 Official school sites must be created according to the requirements provided by the Marketing Department. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

15.13 Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites. We are responsible for the safeguarding and protection of children.

16. Mobile Phones and Personal Devices

16.1 While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make users more vulnerable to cyber bullying;
- Can be used to access inappropriate internet material;
- Can be a distraction to learning;
- Are valuable items that could be stolen, damaged, or lost; and

- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

16.2 Windlesham has a no mobile phone policy for pupils. There is poor phone coverage at Windlesham, with very poor/negligible 3G or 4G signal at Windlesham House School. International pupils are allowed to travel to the School with a mobile phone or personal devise, however, on entering the School building, devices must be handed over to the front office for secure storage. Devices are not returned until the pupil returns home.

16.3 Staff Mobile phones

- Subject to the bullet point below, Staff mobile phones must be turned off, must be not carried around in staff pockets and should be left with personal belongings in class cupboards.
- When away on:
    - an off-site school trip;
    - a sports fixture or match,

  staff are permitted to have their mobile devices switched on and on their person. Staff are to only use their mobile devices for phone calls in case of emergency. The School may need to contact the member of Staff to pass on any urgent or emergency message.
- In the prep school, staff mobile phones / personal devices must only be used to access emails in staff areas and not in the presence of children.
- Cameras, iPads, personal devices and mobile phones are prohibited in the toilets or changing areas.

16.4 Visitors may only use their phones outside the building and not in front of children (Please see Data Protection Policy).

17. Mobile Phone or Personal Device Misuse

17.1 Pupils

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy.

17.2 Staff

- Staff are not permitted to use their phones in front of pupils, whilst on the School site (see 16.3.1)
- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment or School iPads will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.

Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the Child Protection and Safeguarding Children Policy, or in the staff contract of employment.

18. iPads

18.1 Make sure that iPads are locked away at the end of the day and that all iPads are accounted for.

18.2 Children are appointed Digital leaders.

18.3 The Head of ICT regularly conducts random searches of school iPad contents, checking that content is appropriate and in accordance with responsible use guidance. In addition, daily reports are provided via Lightspeed detailing suspicious search queries.

18.4 Guidance is provided for pupils and staff in our Acceptable Use Policies.

19. Video Calls

19.1 All boarding children get the opportunity for video calls home each week. Matrons and staff are present to monitor use of equipment used for video calling.

20. Cyberbullying

20.1 Windlesham House takes Cyber bullying (both in and out of school), as with any other form of bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the Anti-Bullying Policy and Child Protection and Safeguarding Children Policy.

20.2 The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

20.3 If an allegation of bullying does occur, the school will:

- Take it seriously;
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully;
- Record and report the incident;
- Provide support and reassurance to the victim;
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

21. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess and conduct a Data Impact Assessment, where necessary (and in accordance with the Data Protection Policy) any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps

up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

22. Protecting Personal Data

22.1 Windlesham believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision. See Data Protection Policy.

22.2 For further information on how we look after your personal data, please refer to our Privacy Policy online and our Data Protection Policy.

23. Remote Access Policy

23.1 Staff are able to access the school network at home via Remote Desktop Protocol (RDP). All users:

- Are able to access a remote desktop session.
- Are able to access the same files and resources as they can when logged onto a school computer on-site.
- Are asked to be vigilant and to log off after use.

24. Reporting on Compliance and Effectiveness

24.1 An annual report, covering compliance with and summaries of:

- The daily reports received (at 7am) by the Head of ICT, showing the previous day's activity with children using the computers, so that any issues can be quickly investigated; examples include:
- Any suspicious search queries using Google.
- The length of time each child spent using the Internet.
- Any suspicious words typed on a computer by a child.
- Using the Rewards and Conducts modules in iSAMS, produce a report of any issues involving the children and what action is taken. When an entry is made, this is copied to the child's Tutor and Houseparent and the Head of Discipline.
- Weekly, monthly and annual reports from 'Class Technology Computers' showing the status of the Network Servers.

25. Breaches of Policy

25.1 Any breach of this Policy may lead to disciplinary action being taken against the staff member/s involved up to and including dismissal, in line with the School's Disciplinary Policy and Procedures. Any staff member/s suspected of committing a breach of this policy will be required to cooperate with the School's investigation, which may involve handing over relevant passwords and login details.

25.2 Staff member/s may be required to remove any social media content that the School considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

25.3 Any non-compliance will be taken seriously, logged and investigated appropriately in line with our disciplinary policy.

Annex A

Staff - Acceptable Use of ICT Policy Agreement

1. This policy outlines what are acceptable and unacceptable uses of Information Communications Technology (ICT) facilities within Windlesham House School (Windlesham). It is relevant to pupils, staff, governors and visitors. Whilst we aim to support the full use of the vast educational potential of new technologies we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect pupils, staff and visitors from e-safety incidents and promote a safe e-learning environment for pupils.

2. Windlesham's ICT facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users at Windlesham. This could also lead to breaches of the data protection rights of a number of individuals causing harm to those individuals, and to Windlesham.

3. At Windlesham we believe that pupils should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the ongoing debate about what responsible digital citizenship means and how we can nurture it within our school.

Acceptable use

4. Windlesham's ICT facilities should only be used to support learning, teaching, research, administration and approved business activities of Windlesham. These services may not be used for personal, personal commercial, political, and other such activities unless expressly authorised by Windlesham.

5. Should authorisation be provided permitting other personal, personal commercial, political, or charitable, any such use must not hinder or interfere with an individual's duties and must not prevent the legitimate use of these facilities by others. Users may not use Windlesham's ICT facilities to store personal non-work related information or materials on the ICT facilities (e.g. eBooks, music, home videos, photography), and use of the ICT facilities is provided with no expectation of privacy.

6. Users should therefore engage in safe computing practices by establishing appropriate access restrictions for their accounts by setting a password for their user account, safeguarding their passwords, backing up files, and promptly reporting any misuse or violations of this policy.

7. Users' accounts and passwords must not be shared with anyone. Users are responsible for the security of their passwords and account information. Disclosure of account or password information may result is disciplinary action.

Monitoring of users

8. Windlesham may monitor the usage of any or all IT facilities (including emails and social media) and has access to reports on any internet sites that have been visited. This is irrespective of whether it is for school or personal use, and users should have no expectation of privacy when accessing or using IT systems or services.

9. Monitoring of ICT facilities is performed:
    - To monitor the performance and operation of the ICT facilities;
    - To secure, fix, enhance or as an inherent part of effective and responsible systems development or operation;
    - To collect evidence pertaining to compliance with this policy, and other related policies, regarding the acceptable use of ICT facilities within the school;
    - To investigate or detect unauthorised use of the computing and network facilities of the school;
    - In the interests of national security, as required by law; and
    - To prevent or detect crime, as by required by law.

10. Windlesham reserves the right to inspect any items of computer equipment connected (physically or wirelessly) to the network. Any ICT device connected to Windlesham's network will be removed if it is deemed to be breaching school policy or otherwise interfering with the operation of the ICT facilities.

11. Windlesham will designate Authorised Personnel, usually IT Services or support staff, to be permitted to engage in monitoring and it will be considered a disciplinary offence for anyone to engage in monitoring activities without proper authorisation or monitor areas outside their areas of responsibility.

Unacceptable use

12. Windlesham reserves the right to block, disconnect or otherwise prevent what it considers to be unacceptable use of its ICT facilities. Unacceptable use includes, but is not limited to:
    - All actions or activities that are illegal or in conflict with Windlesham's policies, procedures and processes;
    - Using the ICT facilities for access, creation, modification, storage, download, hosting or transmission of material that could be considered pornographic, offensive, obscene, or otherwise inappropriate, or for placing direct or indirect links to websites which publish or host pornographic, offensive or inappropriate material;
    - Publishing materials or making statements which Windlesham may deem to be advocating illegal activity, or threatening, or harassing, or defamatory, or bullying or disparaging of others, or abusive, or libellous, or slanderous, or indecent, or obscene, or offensive or promotes unlawful discrimination, breaches copyright or otherwise causing annoyance, or inconvenience;

- Unauthorised production, distribution, copying, selling, hiring, performing of copyrighted material including, but not limited to, digitisation and distribution of computer software, television, radio, streaming services, websites, photographs, magazines, books, music or any copyrighted sources and installation of any copyrighted software for which Windlesham does not have an active licence or explicit permission of the copyright owner, is strictly prohibited;
- Authoring or sending any form of electronic communications or messages, including, but not limited to, messages and emails that were unsolicited and may be considered junk mail, "chain letters", "Ponzi", hoax warnings or advertising, and that do not correctly identify you as the sender, or messages which appear to originate from another person;
- Unauthorised transmission, distribution, discussion or disclosure of information gained through a user's presence within Windlesham or through the use of ICT facilities;
- Connecting any non-approved ICT device, system or service (including wireless access points) to school networks or setting up any network services, without the explicit or delegated permission from Authorised Personnel;
- Unauthorised access (or attempted unauthorised access) to any ICT facilities provided by Windlesham;
- Allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the ICT facilities;
- Causing any damage to ICT facilities, including through the consumption of food or drink, or moving or removing such facilities without authorisation. Windlesham House School reserves the right to charge for any damage caused;
- Attempting to modify, alter or in any way interfere with ICT facility security controls, hardware or software, configurations, settings, equipment, data files or websites without the written authorisation or delegated permission from Authorised Personnel;
- Introduction of unauthorised and/or malicious software or programs into the ICT facilities, including, but not limited to: unlicensed software, viruses, worms, Trojan horses or logic bombs; by downloading, creating or using any program, tool or item of software designed to monitor, damage, disrupt or interfere with the functioning of ICT facilities, user accounts or data;
- Effecting security breaches or disruptions of network communication, including, but not limited to, accessing or modifying data (or data headers) of which the user is not an intended recipient or logging into an ICT system or service, or account, that the user is not expressly authorised to access. Disruption includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information;
- Executing any form of network monitoring including any data capture, port scanning or security scanning without written authorisation or delegated permission from Authorised Personnel;
- Registering for any system or service, including, but not limited to, social media accounts, web applications, domain names, which includes the name of Windlesham House School or any similar name, or abbreviation that may mislead the public into believing that the domain name refers to Windlesham; and

- Acting in any way that directly or indirectly causes disruption to others' use of school ICT facilities, or using ICT facilities to disrupt or deny the use of ICT facilities of third parties at any time.

Remote Access

13. Remote access to Windlesham network is possible where this has been granted by IT Services.

14. Remote connections are considered direct connections to Windlesham network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

Staff Resident on Site

15. Resident staff are permitted to use the staff and visitor wi fi networks at all times whilst on site. However, this right is a privilege which can be evoked by the school at any time if it so wishes. Staff are permitted to share access to the visitor wifi to household members and visitors. However, they remain responsible for acceptable use of the network by those persons.

Social Media

16. At Windlesham we recognise that social media and networking are playing an increasing role within everyday life and that many staff are users of tools such as Facebook, Twitter and blogs for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. Staff should apply the provisions of this policy with regard to social networking.

Staff Acceptable Use Agreement:

I understand that I must use Windlesham' 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, including as to the personal data of others. When using Windlesham's ICT facilities:

- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details);
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable to IT Services when I see it online;
- 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 respect others' work and property and will not access, copy, remove or otherwise use or alter any other users' files, without the owner's knowledge and permission, and I will ensure that any use is in accordance with school policies;
- I understand there are risks when using the systems and services, 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 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 respect copyright of materials and intellectual property rights and not take or distribute text, images or other materials without permission;
- I will not use or modify any of Windlesham devices, systems and services in any way that will disrupt their use for others in any way;
- I will not install or attempt to install or store programmes of any type on any Windlesham device, nor will I try to alter computer settings;
- I understand that I am not permitted to attempt to connect any devices or systems (e.g. laptops, mobile phones, USB devices, etc.) to any school devices, systems or services without prior permission from an Authorised Person within Windlesham. I understand that, if I am permitted to use my own devices in Windlesham I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with Windlesham House School's policies. I will not use my personal equipment to record these images, unless I have permission from the school and from the individual to do so;
- I will only use social networking sites in school in accordance with Windlesham's policies;
- I will only communicate with pupils, parents / carers, and other parties solely related to my employment, using official school systems. Any such communication will be professional in tone and manner;
- I will not engage in any online activity that may compromise my professional responsibilities;
- I recognise that a failure to comply with the policies of Windlesham, and any misuse of ICT equipment, could lead to breaches of the rights of data subjects and I will act at all times in accordance with such policies in order to avoid any inappropriate use of personal data, or the breach of the data protection rights of any individual.

I understand that I am responsible for my actions, both inside and outside of Windlesham:

- I understand that Windlesham 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 Windlesham and where they involve my membership of Windlesham community (for example, use of images, digital communications, or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to Windlesham ICT systems and services, disciplinary action as set out in the codes of conduct and in the event of illegal activities involvement of the police.

I agree to follow these guidelines at all times when:

- using or connected to Windlesham's devices, systems and services;
- using my own equipment inside or outside of Windlesham in a way that is related to me being a member of this school (for example, communicating with other members of Windlesham, accessing school email, websites and services).

I have read and understand that use of Windlesham IT systems and devices are governed by this full Acceptable Use Policy Agreement and other related Windlesham policies.

Print Name

Signed

Annex B

Windlesham House School - Technology Rules of the Road (Pupil Acceptable Use Policy Agreement)

1. Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

2. At Windlesham House School (Windlesham), we value the use of Technology to help us with our learning. You will find that there are many different opportunities during the day to use different Digital tools to support your studies. We aim for all our pupils to become effective users of technology and responsible digital citizens.

3. Please review this important agreement related to the use of Technology at Windlesham. It is recommended that you should the read Technology Rules of the Road carefully with your parents. You must place your initials next to each expectation, the completed form can then be returned with your application form. These rules need to be signed before you can use the Internet and will help you to keep safe and to be fair to others.

Aim

This Agreement is intended to make sure that pupils:

- will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use;
- do not put Windlesham systems and users from accidental or deliberate misuse that could put the security of the systems at risk
- have good access to digital technologies to enhance their learning

Pupil's Responsibilities

Pupils should initial next to each responsibility:

Initial	Daily Responsibilities
	I will use technology for educational purposes and approved activities during school hours;
	I will never leave an IT device unattended around the School;
	I will close all programs and log out before leaving the computer.
	I will take care of the computer and other equipment. I will leave the computer and other equipment in the same condition I found it.
	I will keep any iPad I use protected using a case
	I will make sure technology I have doesn't distract me or others in the classroom (sound, screen effects, etc.).
	Pupils being responsible digital citizens
	I will only visit those websites approved by the teacher or directly related to the topic the teacher assigns.

	I will only access the Windlesham network with the login I have been given.
	I will remember to stay on task during class time and use the iPad only for activities the teacher approves.
	If I accidentally visit a website or receive a message with inappropriate or unpleasant content or anything that makes me feel uncomfortable, I will press the back button and immediately report to a teacher. This is to help protect me and other pupils.
	I will not allow anyone else to use an iPad I am given and understand the iPad remains my responsibility
	I will be aware of "stranger danger" when communicating online
	I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, sex, educational details, financial details, password or usernames etc.
	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 give permission for the school to provide and manage a G Suite for Education account in my name. I will use my G Suite account to complete assignments, receive feedback, and learn 21st century digital citizenship skills.
	Security and Integrity of Technology
	Only use my own personal devices in school if I have permission.
	If I do use my own device at School, I will follow the rules set out in this agreement in the same way as if I were 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,
	I will not 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 (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.
	Research and Recreation
	I will make sure 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 using the internet to find information, I will take care to check that the information 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.
	Complying with School systems and procedures
	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.
	I understand that Windlesham will monitor my use of the systems, devices and digital communications.

	I understand that Windlesham 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 (e.g. use of images or personal information).
	I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Signatures

The signature below acknowledge that the pupil has reviewed, understood, and agreed to follow the "Technology Rules of the Road" (Acceptable Use Policy Agreement). If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil
Name and Class (print):

Pupil Signature:

Date:

Parent
Parent or Guardian: I understand the terms and restrictions and authorise the above named pupil to utilise the ICT Facilities at Windlesham House School.

Parent Name (print):

Parent Signature:

Date:

Annex C

Windlesham House School Image Consent Form

Name of child: _____

To comply with the Data Protection Act 2018, we need your permission before we can photograph or make any recordings of your child. Only images of children in suitable dress will be recorded and shared. Please answer the questions below, then sign and date the form where shown and return the completed form to the school. Please note that the first initial of a child's surname may be used to distinguish between two children with the same first name. Please circle your answer.

I give permission for my child's image and first name*, to be used within school for internal displays and on internal display screens.	Yes/No
I give permission for my child's image and first name* to be used in Learning Journeys/Records of Achievements belonging to other children.	Yes/No
I give permission for my child's image and first name* to be used in external marketing materials, e.g. website, social media, newsletter, advertising	Yes/No
I give permission for my child to have their image taken for the local paper/magazine.	Yes/No
I give permission for my child's image to be included in sports teams' photos and accompanied by the initial of their first name and their surname in full. I understand this printed/digital image can be purchased by parents via the school or from the photographer's password-protected website.	Yes/No
I give permission for my child to have a whole school photograph taken. I understand this printed/digital image can be purchased by parents via the school or from the photographer's password-protected website.	Yes/No
I give permission for my child to be in the Leavers' photograph when they reach year 8.	Yes/No
Where I have selected "yes" above, I give permission for my child to have their full name and year group to be included in the photo detailed above.	Yes/No
I give permission for images (including videos) of my child to be used once my child has left Windlesham House School.	Yes/No
I give permission for my child's image to be used on the alumni newsletter and website (access only by OWLS)	Yes/No

* The first initial of a child's surname may be used in order to distinguish between two children with the same name

Parent/guardian signature _____ **Date:** _____

Please print name_____

You are free to withdraw your consent at any time. If you wish to withdraw your consent for any of the above activities, please contact the School Office. If you have any other questions, please get in touch.