



Contents

1. Scope of the Online Safety Policy	2
2. Policy development, monitoring and review	2
3. Responsibilities	2
4. Purpose of the Online Safety Policy	6
5. Acceptable use agreements (Annex 3)	7
6. Reporting and responding	7
7. Online Safety Education Programme	8
8. Contribution of pupils	9
9. Staff	9
10. Governors	10
11. Families	10
12. Technology.....	10
13. Filtering & Monitoring – Provided by SmoothWall	10
14. Technical Security	12
15. Mobile technologies	12
16. Social media	13
17. Digital and video images	14
18. Online Publishing	15
19. Data Protection	15
20. Computer Misuse.....	15
Annex 1 - Online Safety Group Terms of Reference	17
Annex 2 – Using mobile Technologies including Bring Your Own Device (BYOD) Policy	19
Annex 3 – Acceptable Use Agreements	22

1. Scope of the Online Safety Policy

- 1.1 This Online Safety Policy outlines the commitment of Windlesham House School (“the School”) to safeguard members of our school community online, in accordance with statutory guidance and best practice.
- 1.2 This Online Safety Policy applies to all members of the school community (including staff, pupils, EYFS pupils, after-school care, governors, volunteers, parents and carers, visitors, and community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).
- 1.3 The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies, and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

2. Policy development, monitoring and review

- 2.1 This Online Safety Policy has been developed by the Head of Digital Learning in conjunction with the Designated Safeguarding Lead (DSL), the Headteacher, Senior Leadership Team, and the Governing Body.
- 2.2 The school will monitor the impact of the policy using:
 - Logs of reported incidents
 - Filtering and monitoring logs
 - Internal monitoring data for network activity
 - Surveys/questionnaires of pupils, parents & carers, and staff
- 2.3 The Governing Body will, as a minimum, receive an annual report on the implementation of the policy. Termly reports to the Governing Body on online safety will be provided under the termly safeguarding report to Governors.

3. Responsibilities

To ensure the online safeguarding of members of our school community, it is important that all members of that community work together to develop safe and responsible online behaviours. This includes learning from each other and from good practice elsewhere, and reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

3.1 Headteacher and senior leadership team

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in *Keeping Children Safe in Education*.
- The Headteacher, the DSL, and the Bursar are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher and SLT are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Headteacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Headteacher and SLT will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The Headteacher and SLT will work with the responsible Governor, the designated safeguarding lead (DSL), and IT service providers in all aspects of filtering and monitoring.

3.2 Governors

3.2.1 Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The Governing Body will receive termly reports on online safety.

3.2.2 A member of the Governing Body will take on the role of Online Safety Governor to include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Checking that provision outlined in the Online Safety Policy (e.g., online safety education provision and staff training) is taking place as intended
- Ensuring that the filtering and monitoring provision is reviewed and recorded at least annually (the review will be conducted by members of the SLT, the DSL, and the IT service provider, and involve the responsible governor)
- Reporting to relevant governors group/meeting
- Receiving relevant training
- Membership of the school Online Safety Group

3.2.3 The Governing Body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

3.3 Designated Safeguarding Lead (DSL)/Online Safety Lead

The DSL will:

- Hold the lead responsibility for online safety within their safeguarding role
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up-to-date capability required to keep children safe whilst they are online
- Meet regularly with the online safety governor to discuss current issues, review incidents and filtering and monitoring logs, and ensure that annual filtering and monitoring checks are carried out
- Attend relevant Governing Body meetings/groups
- Report regularly to the Headteacher and SLT
- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

- Lead the Online Safety Group (see Annex 1)
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns, and ensure that these are logged to inform future online safety developments
- Have a leading role in establishing and reviewing the school online safety policies/documents
- Promote an awareness of, and commitment to, online safety education/awareness raising across the school and beyond by coordinating an online safety education programme across the school years, including themed events
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded, and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/pupils
- Liaise with technical staff, pastoral staff, and support staff
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined in *Keeping Children Safe in Education*: content, contact, conduct, commerce

3.4 Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood, and signed the staff Acceptable Use Agreement (SUA)
- They immediately report any suspected misuse or problem to the school's DSL, online safety lead, and IT Service team for investigation/action, in line with the school safeguarding procedures
- All digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- They ensure pupils understand and follow the Online Safety Policy and acceptable/safe use agreements, have a good understanding of research skills, and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use, and processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- There is a zero-tolerance approach to incidents of online bullying, sexual harassment, discrimination, hatred, etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media

3.5 IT Service Provider (CTS)

3.5.1 It is the responsibility of Windlesham House School to ensure that the IT service provider (CTS) carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider (CTS) follows and implements the school Online Safety Policy and procedures.

3.5.2 The IT Service Provider is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy.
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements.
- There is clear, safe, and managed control of user access to networks and devices.
- 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.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action.
- The filtering policy is applied and updated on a regular basis, and its implementation is not the sole responsibility of any single person.
- Monitoring systems are implemented and regularly updated as agreed in school policies.

3.6 Pupils

- Are responsible for using the school digital technology systems in accordance with the pupil Acceptable User Agreement and Online Safety Policy.
- Should understand the importance of reporting abuse, misuse, or access to inappropriate materials, and know how to do so.
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school if related to their membership of the school.

3.7 Parents and carers

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

- Publishing the school Online Safety Policy on the school website.
- Providing them with a copy of the pupils' acceptable use agreement.
- Publishing information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images.
- Workshops, newsletters, website, social media, and information about national/local online safety campaigns and literature.

3.7.2 Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to pupils in school.
- The safe and responsible use of their children's personal devices in the school.

3.8 Community users

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

3.9 Online Safety Group (Annex 1)

3.9.1 The Online Safety Group has the following members:

- Designated Safeguarding Lead/Online Safety Lead
- Senior leaders
- Online safety governor
- Technical staff
- Teacher and support staff members
- Pupils

3.9.2 Members of the Online Safety Group will assist the DSL/Head of Digital Learning with:

- The production/review/monitoring of the school Online Safety Policy/documents.
- The production/review/monitoring of the school filtering policy and requests for filtering changes.
- Mapping and reviewing the online safety education provision – ensuring relevance, breadth, progression, and coverage.
- Reviewing network/filtering/monitoring/incident logs, where possible.
- Encouraging the contribution of pupils to staff awareness, emerging trends, and the school online safety provision.
- Consulting stakeholders – including staff/parents/carers – about the online safety provision.
- Monitoring improvement actions identified through use of the 360-degree safe self-review tool.

3.9.3 An Online Safety Group terms of reference template can be found in the appendices.

4. Purpose of the Online Safety Policy

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- Allocates responsibilities for the delivery of the policy.
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school, and how they should use this understanding to help safeguard pupils in the digital world.
- Describes how the school will help prepare pupils to be safe and responsible users of online technologies.
- Establishes clear procedures to identify, report, respond to, and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- Is supplemented by a series of related acceptable use agreements.

- Is made available to staff at induction and through normal communication channels.
- Is published on the school website.

5. Acceptable use agreements (Annex 3)

- 5.1 The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/reinforced through:
- Staff induction and handbook.
 - Digital signage.
 - Communication with parents/carers.
 - Built into education.
 - School website.
 - Peer support.
- 5.2 When using communication technologies, the school considers the following as good practice:
- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
 - Any digital communication between staff and pupils or parents/carers must be professional in tone and content.
 - Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
 - Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening, or bullying in nature, and must not respond to any such communication.

6. Reporting and responding

- 6.1 The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school, which will need intervention.
- 6.2 The school will ensure:
- There are clear reporting routes which are understood and followed by all members of the school community, which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints, and managing allegations policies.
 - All members of the school community will be made aware of the need to report online safety issues/incidents.
 - Reports will be dealt with as soon as is practically possible once they are received.
 - The Designated Safeguarding Lead/Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
 - If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures.
 - Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of the Governing Body.

- Where there is no suspected illegal activity, devices may be checked using the following procedures:
 - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - Conduct the procedure using a designated device that will not be used by pupils, and if necessary, can be taken off-site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
 - Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures.
 - Involvement by local authority.
 - Police involvement and/or action.
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- Incidents should be logged.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow-up actions.
- Learning from the incident (or pattern of incidents) will be provided to the school community to support online safety development.

6.3 The school will treat online safety incidents the same as safeguarding and therefore implement the decision-making process for dealing with incidents. However, in this instance the Head of Digital Learning will also be included in the process.

6.4 Incidents that involve inappropriate or illegal misuse are dealt with as soon as possible in a proportionate manner. Members of the school community will be made aware that the incident has been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

7. Online Safety Education Programme

7.1 Online safety should be a focus in all areas of the curriculum, and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant, and provide progression, with opportunities for creative activities, and will be provided in the following ways:

- A [planned online safety curriculum](#) for all year groups matched against a nationally agreed framework (Common Sense Media).
- Lessons are matched to need, are age-related, and build on prior learning.

- Lessons are context-relevant, with agreed objectives leading to clear and evidenced outcomes.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas, e.g., PHSE.
- The programme will be accessible to pupils at different ages and abilities.
- Vulnerability is actively addressed as part of a personalised online safety curriculum.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet, and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use, and that processes are in place for dealing with any unsuitable material found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for need.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

8. Contribution of pupils

The school acknowledges, learns from, and uses the skills and knowledge of pupils ('Pupil Voice') in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people.

9. Staff

9.1 All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme, issued by the DSL, of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- The training will be an integral part of the school's annual safeguarding and data protection training for all staff.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation, and the need to model positive online behaviours.
- This Online Safety Policy and its updates will be presented to staff.

10. Governors

- 10.1 Governors should take part in online safety training/awareness sessions. This may be offered through participation in school training/information sessions for staff.
- 10.2 A higher level of training will be made available to (at least) the safeguarding lead Governor. This will include training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

11. Families

The school will seek to provide information and awareness to parents and carers through:

- Regular communication, awareness-raising, and engagement on online safety issues, curriculum activities, and reporting routes.
- Regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carers evenings, etc.
- The pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by pupils leading sessions at parent/carers evenings.
- Letters, newsletters, website, and learning platform.
- Reference to the relevant websites/publications and training.

12. Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

13. Filtering & Monitoring – Provided by SmoothWall

- 13.0.1 The school filtering and monitoring provision is agreed by senior leaders, governors, and the IT Service Provider (CTS), and is regularly reviewed and updated in response to changes in technology and patterns of online safety incidents.
- 13.0.2 The DSL will have lead responsibility for safeguarding and online safety, and the IT service provider will have technical responsibility.
- 13.0.3 Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead, and a governor, in particular when a safeguarding risk is identified.

13.1 Filtering

- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the

standards defined in the DfE [Filtering standards for schools and colleges](#) and the guidance provided in the UK Safer Internet Centre [Appropriate filtering](#).

- Illegal content is filtered by the filtering provider SmoothWall.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- The school has provided differentiated user-level filtering.
- Younger pupils will use safe search engines.
- Access to content through non-browser services (e.g., apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

13.2 Monitoring

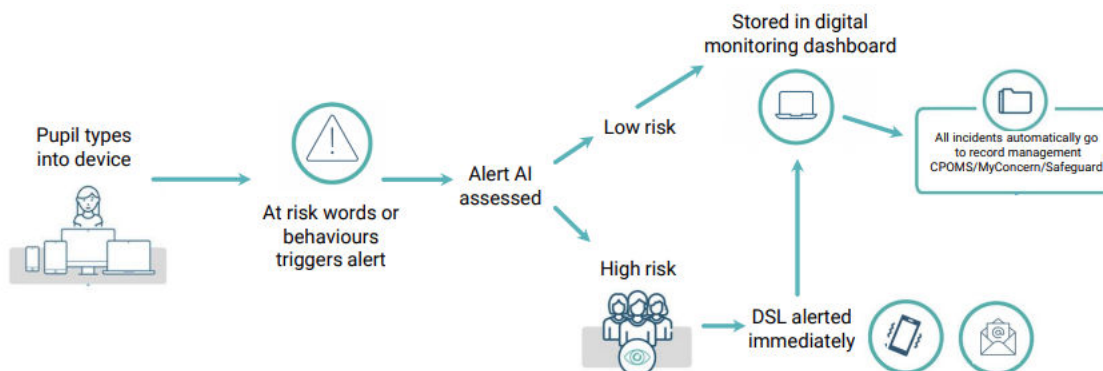
13.2.1 The school has monitoring systems in place to protect the school, systems, and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on, and outcomes are recorded by the Designated Safeguarding Lead; all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

13.2.2 The school follows [Appropriate Monitoring](#) guidance and protects users and school systems through the use of the appropriate blend of strategies. These may include:

- Physical monitoring.
- Internet use is logged, regularly monitored, and reviewed.
- Filtering logs are regularly analysed, and breaches are reported to DSL.
- Proactive alerts inform the school of breaches to the filtering policy, allowing effective intervention.

Digital monitoring - how it works - Smoothwall only



14. Technical Security

- The school technical systems will be managed in ways that ensure the school meets recommended technical requirements.
- Responsibility for technical security resides with SLT, who may delegate activities to identified roles.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed at least annually by the SLT/Online Safety Group.
- Password policy and procedures are implemented.
- The security of their username and password must not allow other users to access the systems using their log-on details.
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log-on details.
- All school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- The administrator passwords for school systems are kept in a secure place.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, and devices from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- The Head of Digital Learning is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates are applied.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software on school-owned devices without the consent of the IT service provider.
- Systems are in place to control and protect personal data, and data is encrypted at rest and in transit.
- Mobile device security and management procedures are in place.
- Guest users are provided with appropriate access to school systems based on an identified risk profile.

15. Mobile technologies

The school acceptable use agreements (Annex 3) for staff, pupils, parents, and carers outline the expectations around the use of mobile technologies. In addition to this, please see Annex 2 – Using Mobile Technologies, including Bring Your Own Device Policy.

15.1 School-owned/provided devices:

- All school devices are managed through the use of Mobile Device Management software.
- There is an asset log that clearly states whom a device has been allocated to.
- Personal use is clearly defined, and expectations are well-communicated.
- The use of devices on trips/events away from school is clearly defined, and expectations are well-communicated.
- Liability for damage aligns with current school policy for the replacement of equipment.
- Education is in place to support responsible use.

15.2 Personal devices:

- Pupils are not permitted to use personal mobile phone devices during the school day.
- There is a clear policy on the use of personal mobile devices by boarding pupils.
- There are clear rules on the use of personal mobile devices by staff in the Staff Code of Conduct.
- Where personal devices are brought to school but their use is not permitted, appropriate, safe, and secure storage is available via the school office.
- Use of personal devices for school business is defined in the acceptable use policy and staff handbook.
- The expectations for taking, storing, and using images/video align with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- Education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

16. Social media

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

- Ensuring that personal information is not published.
- Education/training being provided, including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection, and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Guidance for pupils and parents/carers.

16.0.2 School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers, or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media.

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

- A process for approval by senior leaders.

- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

16.1 *Personal use*

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

16.2 *Monitoring of public social media*

- As part of active social media engagement, the school may proactively monitor the Internet for public postings about the school.
- The school will effectively respond to social media comments made by others via the Head of Marketing.
- When parents/carers express concerns about the school on social media, we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

17. *Digital and video images*

- The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.
- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance/policies.
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication, and distribution of images.
- Staff/volunteers must be aware of those pupils whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- Parents/carers are welcome to take videos and digital images of their children only at school events for their own personal use. To respect everyone's privacy, and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims but must follow school policies concerning the sharing, storage, distribution, and publication of those images.

- Care should be taken when sharing digital/video images that pupils are appropriately dressed.
- Pupils must not take, use, share, publish, or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils, will be selected carefully and will comply with the Online Safety Policy.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored, and for how long – in line with the school data protection policy.
- Images will be securely stored in line with the school retention policy.

18. Online Publishing

- 18.1 The school communicates with parents/carers and the wider community and promotes the school through:
- Public-facing website.
 - Social media.
 - Online newsletters.
- 18.2 The school website is managed by the Head of Marketing. The school ensures that the online safety policy has been followed in the use of online publishing, e.g., use of digital and video images, copyright, identification of young people, publication of school calendars, and personal information – ensuring that there is least risk to members of the school community through such publications. Where pupil work, images, or videos are published, their identities are protected, and full names are not published.

19. Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation and the School Data Protection Policy.

20. Computer Misuse

- All key stakeholders, including the school IT service provider CTS, have responsibility for the safeguarding of young people from computer misuse.
- The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue.
- All staff are made aware of the safeguarding risks of computer misuse.
- Learners agree to the Acceptable Use Agreement (AUA), which outlines acceptable online behaviours and explains that some online activity is illegal.
- Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online.

- Any breach of the AUA or activity by a learner that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead (DSL, Jim Taylor) for consideration as a safeguarding risk.
- Where the DSL believes that the learner may be at risk of committing cybercrimes, or already be committing cybercrimes, a referral to the local [Cyber Choices](#) programme will be made. Where the DSL is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team.
- Parents also have the opportunity to report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSL.
- The IT service provider, CTS, is aware of the safeguarding requirement to refer concerns about computer misuse to the Designated Safeguarding Lead and has a clear process to follow in order to do so.

Annex 1 - Online Safety Group Terms of Reference

(Last approved by the Governing Body 23 September 2025)

1. Purpose

To provide a consultative group that has wide representation from the schools community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. Membership

The online safety group will seek to include representation from all stakeholders. The composition of the group will comprise

Designated Safeguarding Lead/Head of Online Safety
Head of Digital Learning
Compliance Officer
Teaching staff Member
ICT technical staff including the infrastructure manager
Governor
Digital Learner pupil representatives x 2

Other people may be invited to attend the meetings at the request of the Chair on behalf of the committee to provide advice and assistance where necessary.

Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chair

The Designated Safeguarding Lead/Head of Online Safety will Chair the group. Their responsibilities include:

- Scheduling meetings and invitations to meetings
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that meeting notes are taken, with action points and distributed as necessary

4. Duration of Meetings

Meetings shall be held as a minimum termly. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through
 - Staff training/meetings/briefings
 - Learner forums (for advice and feedback)
 - Governor meetings
 - Surveys/questionnaires for learners, parents/carers and staff
 - Parent/carer sessions
 - Website/Newsletters
 - Online safety events
 - Internet Safety Day (annually held on the second Tuesday in February)
 - With the IT Service Provider and Governor, to carry out checks on filtering and monitoring systems
 - To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
 - To monitor incidents involving online bullying

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority. The above Terms of Reference for Windlesham House School have been agreed

Annex 2 – Using mobile Technologies including Bring Your Own Device (BYOD) Policy

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network.

The primary purpose of having a personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned.

Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximising the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high tech world in which they will live, learn and work.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset.

- The school acceptable use agreements for staff, learners and parents/carers will give consideration to the use of mobile technologies
- The school allows:

	School/devices		Personal devices			
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device ¹	Learner owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access						
Internet only	Yes	Yes	Yes	Yes	Yes	Yes
No network access						

1. Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

Windlesham House School has provided technical solutions for the safe use of mobile technologies on and off campus:

- All school devices are managed by CTS, though the use of Mobile Device Management software - Microsoft Intune.
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access).
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
- For all mobile technologies on the school network, filtering (SmoothWall) will be applied to the internet connection and attempts to bypass this are not permitted.
- Appropriate exit processes, managed by CTS, are implemented for devices no longer used at a school location or by an authorised user. These include; revoking the link between MDM software and the device and uninstalling school-licensed software etc.
- All mobile devices on the school network are monitored.
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices can be made to ensure that users have not removed required apps.
- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Where a school device has been provided to support learning. It is expected that learners will bring devices to the school as required and keep in good condition.
- The changing of settings that would stop the device working as it was originally set up and intended to work is not permitted.

When personal devices are permitted:

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device into the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security.
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device or the resolution of hardware issues

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition:

- Devices are not permitted in tests or exams.
- There is clear advice and guidance at the point of entry for visitors to acknowledge school requirements.
- Users are responsible for keeping their device up to date through software, security and app updates.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- Confiscation and searching as per the school searching pupils and their possessions policy - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions.
- Printing from personal devices will not be possible

Insurance

Our IT Services provider, Class Technology Solutions (CTS), working in partnership with The Rent Company (TRC), can provide an end-to-end device procurement process, specially designed for parents and pupils. The Easy4u subscription guarantees worry-free computing. The standard package includes a support service, warranty extension, a protective sleeve and damage and theft insurance.

Annex 3 – Acceptable Use Agreements

ACCEPTABLE USE AGREEMENT - STAFF

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

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.
- I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology.
- I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. Nor will I share passwords such as wifi with pupils.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are
- published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with staff, learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, 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 ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) 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 not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Acceptable Use Agreement 2025-2026 (Senior)

Digital technologies can greatly enhance our learning at Windlesham House School and have become an integral part of our daily lives. With the many benefits technology brings, it is crucial, however, that we use these resources safely and responsibly. At Windlesham House School we want you to become effective users of technology and responsible digital citizens. Thus, we've created the following user agreement for you to follow and so you are aware of what is expected of you.

Read this user agreement carefully so you are aware what is expected of you.

- Once you understand what is expected of you in each section, please check the box 'I agree'.
- By checking 'I agree', this is your commitment to adhering to these expectations, your readiness to utilise digital resources and to maintain a safe and respectful digital environment.

I understand how to complete this user agreement form.

☐

What is the objective of this Acceptable Use Agreement

This form ensures that:

- You understand our expectation and act as a responsible user of the internet and digital technologies for educational, personal, and recreational use.
- You understand that I must use school systems in a responsible way, to ensure you avoid actions that may harm yourself, others, the wider community and put the security of Windlesham's systems at risk.
- You utilise digital technology and resources to enhance your learning.

I understand

☐

Daily Responsibilities:

- I will use technology for educational and approved activities during school hours.
- I will never leave a device unattended on school premises.
- I will properly shut down all programs and log out before leaving a desktop.
- I will respect and care for all technological devices and leave them as I found them.
- I will ensure any iPad I use is protected with a case.
- I will ensure technology (sound, screen effects etc) does not distract me or others in the classroom.
- If I damage or notice damage to a digital device I will report it to a member of staff.
- I understand that if I purposely damage a school device, I may have to pay to fix or replace.

I agree

☐

Being Responsible Digital Citizens:

- I will visit only those websites approved by the teacher/the school or relevant to assigned topics.
- I will only use my assigned login to access the Windlesham network.
- I will stay focused and stay on task during class, using the technology and/or my digital device only for approved activities.
- I will report any accidental access to inappropriate or uncomfortable content to a member of staff immediately.
- I will not allow anyone else to use my assigned digital device and accept responsibility for it.
- I will be conscious of "stranger danger" if communicating online.
- I will not share personal information (names, address, phone numbers etc) about myself or others online.
- I will respect others' work and not tamper with others' files without permission.
- I will communicate politely and respectfully, understanding others may have different opinions.
- I will use my Google Suite account responsibly to complete assignments and learn digital citizenship skills.
- I give permission for the school to provide and manage a Google Suite for Education account in my name.

I agree

☐**Security and Integrity of Technology:**

- I will only use my personal devices in school with permission and if I do use my own device I will adhere to the expectations set in this agreement and the mobile device policy.
- I will not upload, download, or access harmful, inappropriate, or illegal material.
- I will not attempt to bypass any monitoring, filtering or security systems.
- I will promptly report any damage or issues with equipment or software.
- I will open email attachments or hyperlinks only from known, trusted sources, I will check with a member of staff if unsure.
- I will not install or store programs on any school device or alter computer settings

I agree

☐**Research and Recreation:**

- I will respect copyright laws and obtain permission to use others' work.
- I will not download copyrighted materials.
- I will verify the accuracy of online information with other sources and keep aware of the potential misleading content available to me.

I agree

☐

Complying with School Systems and Procedures:

- I will use digital systems and resources responsibly to ensure no risk to my safety and the safety and security of others.
- I understand that Windlesham will continuously monitor my use of systems, devices, and digital communications.

I agree☐**Use of AI:**

- Only use AI to generate material as instructed by my teacher and relevant to assigned topics.
- I will be clear and transparent about where AI has been used within the creation of my work.
- I will not use AI to generate material and submit it as my own.
- I will comply with laws, regulations, policies and guidelines when using AI generated material.

I agree☐**Responsibility for my actions both in and out of school:**

- I understand that Windlesham House School 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.
- I understand that failure to comply with this agreement may lead to disciplinary actions, including loss of network and device access, contact with parents, or involvement of the police if deemed necessary.

I agree☐

Please sign and date below to show that you have read, understood and agree to the above conditions of use.

Name: _____

Form: _____

Date: _____

Acceptable Use Agreement 2025-2026 (Junior)

Technology like computers, the internet and AI can help us learn at Windlesham House School. We need to use all technology carefully and responsibly. This agreement explains how you should and how we expect you to use technology at school.

Please read this form carefully so you are aware what is expected of you.

- If you understand and agree to follow these expectations, check 'I agree' after each section.
- This shows you will use technology properly and help keep Windlesham's systems safe.

I understand how to complete this user agreement form.

☐

What is the point of this user agreement?

- It helps you use the internet and technology responsibly at school and home.
- It helps you avoid actions that could harm you, others or Windlesham's systems.
- It supports you to use technology to learn new things.

I understand

☐

What I will do every day:

- Only use technology for schoolwork during school hours.
- Never leave a computer or device unattended.
- Properly shut down and log out when I have finished.
- Be gentle with all devices and leave them how I found them.
- Make sure any iPad I use has a case to protect it.
- Make sure technology doesn't distract me or others.
- If I damage or notice damage to a digital device I will report it to a member of staff.
- If I purposefully damage a school device, I know I may have to pay to replace or fix it.

I agree

☐

Being a responsible technology user:

- Only visit websites as instructed by my teacher.
- Only use my own login for Windlesham computers.
- Stay focused on tasks; only use digital devices for schoolwork.
- Tell a teacher if I see anything bad online, even as an accident.
- Not let others use my digital device
- Take care of the digital device I am using.
- Only talk online to people I physically know and check before doing so.
- Not share personal information online.
- Not change others' work without asking first.
- Be polite online and listen to different opinions.
- Use my Google Suite responsibly to do assignments and learn.

I agree

☐

Keeping technology secure:

- Only use my own devices at school if I get permission first and follow these rules and the mobile device policy.
- Not download or access anything dangerous, wrong or illegal, report it to staff if I do, even accidentally.

- Not try to get around monitoring, filters or security.
- Tell someone if any technology is damaged or not working.
- Only open emails and links from people I know, and check if unsure.
- Not install programs or change settings on school devices.

I agree

☐

Research and fun:

- Respect copyright and get permission to use others' work.
- Not download copyrighted materials.
- Check accuracy of online information in other places to make sure it's true.

I agree

☐

Use of AI:

- Only use AI to generate material as instructed by my teacher.
- Explain where AI has been used within the creation of my work.
- Not use AI to generate material and submit it as my own.
- Comply with laws, regulations, policies and guidelines when using AI generated material.

I agree

☐

Following Windlesham's expectations:

- Use technology responsibly to keep myself and others safe.
- Know Windlesham staff can check my use of devices and online activity.

I agree

☐

My actions in and out of school:

- I understand breaking these expectations inside or outside of school. may mean losing computer access, detention, contacting my parents, or getting the police involved.

I agree

☐

Please sign and date below to show that you have read, understood and agree to the above conditions of use.

Name: _____

Form: _____

Date: _____

ACCEPTABLE USE AGREEMENT 2024-2025 (PRE PREP)

Computers and the internet can help us learn at Windlesham House School. We need to be responsible when using technology. This agreement shows how you should use technology at school.

If you understand and agree to follow these expectations, tick the box next to each statement. This shows you will use technology carefully.

What this does:

- Helps you use the internet and computers properly at school and home.
- Avoids actions that could upset or harm you, others or the school's computers.
- Helps you use technology to learn new things.

☐

I understand

What I will do every day:

- Only use technology for schoolwork during school.
- Never leave a computer or device alone.
- Properly turn off and log out when I'm done.
- Be gentle with all devices.
- Make sure technology doesn't distract me or others.

☐

I agree

Being responsible with technology:

- Only go to websites my teacher says I can.
- Only use my own login on school computers.
- Stay focused on work; only use iPads for schoolwork.
- Tell the teacher if I see anything bad online.
- Not let others use my iPad.
- Do not talk to people online.
- Not share personal information online.
- When we do online teamwork activities, I must be polite and listen to others.

☐

I agree

Keeping technology safe:

- Only use my own devices at school if allowed and follow the expectations.
- Not download or access anything dangerous or wrong.
- Tell someone if any technology breaks or does not work.
- Only open emails and links from people I know.

☐

I agree

Research and fun

- Ask permission to use others' work.
- I will not download things.
- Check online information to make sure it's true.

☐

I agree

Use technology responsibly to keep safe.

- I know the school checks my use of devices and online activity.

☐

I agree

My actions in and out of school:

- I understand not meeting these expectations, inside or outside of school, may mean
- losing my go on computers and devices, maybe going to see the Headteacher
- contacting my parents, or other important people.

☐

I agree

ACCEPTABLE USE AGREEMENT 2024-2025 - COMMUNITY USERS

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

- I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:
- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) 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 illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to Others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will 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 download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.