GEORGE ABBOT SCHOOL

Policy Title:	**E-Safety Policy**
Author:	**Designated Safeguarding Lead and Lead for Online Safety**
Date of most recent review:	**Spring 2026**
Date of next review:	**Spring 2027**
School Mission Statement: Academic excellence within a strong community of equality and respect, where potential and opportunity are realised.	

1. Aims of this policy:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- Promote a culture of open communication where students feel safe to talk about their online lives before issues escalate
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Recognise the importance of digital habits, wellbeing and balance not just access and restriction.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, such as computers, mobile phones or games consoles.
- George Abbot identifies that the Internet and information communication technologies are an important part of everyday life so students must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
- The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
  - Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
  - Contact: being subjected to harmful online interaction with other users; for example: Child to Child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
  - Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
  - Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- This policy must be read in conjunction with other relevant George Abbot policies including (but not limited to) Child Protection and Safeguarding Policy, Anti-bullying, Behaviour, Trust Staff Code of Conduct Policy, Relationships and Sex Education and Health Education (RSE), Keeping Children Safe in Education 2025 and Children's Commissioner Report.
- Where children need to learn online at home, due to illness or self-isolation in response to coronavirus, George Abbot will follow expectations as set out within the Child Protection and Safeguarding Policy and in line with DfE Guidance, 'Safeguarding and remote education' 2023.

2. Roles and responsibilities

2.1 The Senior Leadership Team:

- Ensure that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensure that there are appropriate and up-to-date policies regarding online safety.
- Provide students with safe, reliable and useful IT resources.
- Ensure that online safety is embedded within the curriculum, which enables all students to develop an age-appropriate understanding of online safety.

- Ensure there is robust staff training for reporting of concerns, including online safety concerns, on CPOMS, the safeguarding reporting tool.
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.
- Recognise the impact of screen time on sleep, concentration, mood and mental health.
- Ensure online safety is approached as both safeguarding and wellbeing issues- digital habits and safety, sleep, scrolling habits and addiction.

2.2 The Designated Safeguarding Lead and Lead for Online Safety

Details of the school's DSL and Central Safeguarding Team are set out in our Child Protection and Safeguarding Policy. The DSL and Lead for Online Safeguarding takes lead responsibility for online safety in school, in particular:

- Act as a named point of contact on all online safety issues and liaise with other members of staff and agencies to address any online safety issues or incidents.
- Manage all online safety issues and incidents in line with the school Child Protection and Safeguarding Policy.
- Ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with the Child Protection and Safeguarding Policy.
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy and anti-bullying policy.
- Deliver staff training on online safety in accordance with 'Keeping Children Safe in Education' (KCSIE) 2025, 2019 DfE guidance document 'Teaching Online Safety in Schools' and the Children's Commissioner Report.
- Keep up-to-date with current research, legislation and trends.
- Promote online safety to students, staff, parents and guardians.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep students safe online.
- Ensure guidance and policies for online usage of school equipment is up-to-date, that all students follow George Abbot Student Acceptable Use Agreement (Appendix 1), IT Equipment Loan Policy (Appendix 2).
- Support the school community in understanding how AI may impact children's online experiences.
- Use safeguarding data to identify patterns of concern linked to online behaviour including mood, behaviour and engagement.

2.3 The IT Director and Data Protection officer

- Puts in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material, sexually explicit content, violent or graphic content.
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conduct a full security check and monitoring the school's ICT systems on a regular basis.
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- All user activity is monitored using the Securus Full Monitoring Service system. All incidents are reviewed and any online safety incidents are reported to the Central Safeguarding Team to be logged and dealt with appropriately in line with this policy.
- Provide students with IT Equipment Loan Policy (Appendix 2) and ensure compliance through the monitoring of school issued equipment at home.

2.4 All staff

- Maintain an understanding of this policy and implement it consistently.
- Agree and adhere to the terms on the Trust Staff Code of Conduct Policy and ensure that students follow George Abbot Student Acceptable Use Agreement (Appendix 1).
- Work with the DSL to ensure that any online safety incidents are logged on CPOMS in accordance with our Child Protection and Safeguarding Policy and dealt with appropriately in line with this policy.
- Be vigilant to changes in mood, behaviour, sleep, mental health and anxiety and understand the links of these to children's online lives.

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

2.5 Parents/Carers

- Read George Abbot's Student Acceptable Use Agreement (Appendix 1) and encourage their children to adhere to it and adhere to it themselves where appropriate.
- Support George Abbot's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Identify changes in behaviour that could indicate that their child is at risk of harm online, and to seek help and support from George Abbot, or other appropriate agencies, if they or their child encounters online problems or concerns.
- To report any known issues as soon as possible.
- Build healthy routines, including phone free spaces and phone free time at home.
- Engage in regular, open conversations about online experiences both positive and negative
- Be proactive in discussing screen use, sleep, online habits and peer pressure.

2.6 Students

- Read George Abbot Student Acceptable Use Agreement (Appendix 1) and adhere to it.
- Ensure the safety and security of themselves, others, and the school system for all online activity.
- Respect for all members of our community both on and offline.
- Maintain the reputation of the school.
- Year 7-11 are not to use mobiles phones on school site during school hours 08.30am-3.15pm.
- Students must not digitally document or live stream anything whilst on school premises.
- Sixth Form students may use phones inside the Sixth Form buildings only.
- Understand that school owned, and managed IT devices and connected personal IT devices/networks must not be used for any illegal, obscene, offensive, profit making or commercial purpose or for anything other than school business.
- Speak with trusted adults in school or outside is something online makes them feel uncomfortable, worried or upset.

3. Education

3.1 Students

Students will be taught about online safety as part of the curriculum. All schools have to teach Relationships and Sex Education and Health Education (RSE) in secondary schools, as well as PSHE, cyber-bullying, scam and fraud. This encompasses healthy and positive relationships and how students should conduct themselves when online, including sexual harassment, youth produced sexual imagery, sexting, online child sexual abuse and exploitation (including child criminal exploitation).

Students understand how to use devices, networks, the internet and email, safely, responsibly and legally:

- Students understand prolonged periods of time looking at a screen can be harmful and should therefore self-manage regular breaks. No phone policy for Year 7-11 to support. Year 7 and Year 8 Phone Pouches introduced with signal blocking. Confiscation of mobile if seen for Year 9-11.
- Sixth Form are granted access to mobile phones during school day but should only be used within the Sixth Form building or with permission from their class teacher.
- Students can use email/electronic communication responsibly and always be polite and respectful.
- Students understand how to use the internet/devices/apps safely and know the dangers involved when sharing data, using on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).
- Develop strategies for digital free time.
- Develop positive digital habits to manage sleep, mood, focus and maintain good mental health.
- Think critically about AI-generated content and misinformation.

By the end of secondary school, students will:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.

- Recognise inappropriate content, contact and conduct, and know how to report concerns.
- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- Understand how to report a range of concerns.
- Know their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- Know about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Understand not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- Know what to do and where to get support to report material or manage issues online.
- Understand the impact of viewing harmful content.
- Understand that specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- Understand that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- Understand how information and data is generated, collected, shared and used online.
- Understand how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- Understand how people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).
- Understand appropriate, ethical and safe use of AI

3.2 Parents

The school will raise parents' awareness of online safety in the Parent Bulletin or other communications home, and in information via our website. Parent information evenings will be delivered by pastoral teams to include online safety, mobile phone safety and artificial intelligence information to support parents at start of the academic year. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher and/or the DSL (Tracy Young: dsl@georgeabbot.surrey.sch.uk).

4. Staff Code of Conduct for ICT and Social Media

This policy applies to any social communication platform and personal web space used on phones, consoles, tablets and computers.

The internet changes quickly and it is impossible to list every type of communication online. The content within this policy must be followed irrespective of medium.

Staff should be aware that their social media profile, presence and conduct online could compromise their position within the school in relation to the protection of children, loss of trust and confidence or bringing the employer into disrepute. It could also result in action by regulatory bodies.

4.1 School ICT Acceptable Use

All school staff must agree to the following:

- To take responsibility for all activity that takes place under their login on their device, whether owned by the school or personally.
- Passwords must be kept confidential and changed when requested to.
- School devices must not be used by non-school employees.
- Unattended devices, including work desktops, must be locked by pressing 'windows + L'.
- School personal devices must not be left unattended in vehicles.
- Personal email and internet use is only allowed in non-curriculum time and when no students are present.
- Staff will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and viewing pornography or other inappropriate content.

- Not to try to bypass the school's filtering or monitoring system.
- Any personal transaction using the school system is the responsibility of the individual, not the school.
- All files downloaded from the internet, received via e-mail or on removable media (e.g. Data Stick, CD) must be checked for any viruses using the school anti-virus software before use.
- Follow GDPR procedures when using AI tools to support schoolwork

4.2 Computer Viruses and Ransomware

All files downloaded from the internet, received via e-mail or on removable media (e.g. Data Stick, CD) must be checked for any viruses using the school anti-virus software before use. Staff should never interfere with any anti-virus software installed on school ICT equipment. The school antivirus solution is configured so updates will occur when an Internet connection is available.

If staff suspect there may be a virus on any school ICT equipment, they should stop using the equipment and contact the Network Team immediately. The Network Team will advise what actions to take and will be responsible for advising others that need to know. The school has protection in place for ransomware attacks which will protect school hardware whether in school or at home. If staff have any concerns, please contact the Network Helpdesk.

4.3 Monitoring and Filtering of Internet Use

George Abbot School monitors usage of its internet and email services without prior notification or authorisation from users. Users of George Abbot School email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school's ICT system, within the parameters of the law. Should staff receive or inadvertently access inappropriate content, this should be reported to the DSL and network team immediately.

4.4 School Email

Staff should understand that all emails are legally binding and are subject to Data Protection laws. All email correspondence must be professional. Content that could be considered as offensive, rude, defamatory or tarnish the school's reputation must not be sent via email.

Staff must not pass personal data, including anything relating to students, to a third-party individual or organisation.

Staff must ensure that email addresses of parents are not shared with others by using the BCC function.

4.5 Principles of Social Media Use

- Staff must be conscious at all times of the need to keep their personal and professional lives separate. They should not put themselves in a position where there is a conflict between work for the school and personal interests.
- Staff must not engage in activities involving social media which might bring George Abbot School into disrepute.
- Staff must not engage in activities involving social media which conflict with Part Two of the Teachers' Standards.
- Staff must not represent their personal views as those of George Abbot School on any social medium.
- Staff must not discuss personal information about students, George Abbot School staff or other professionals they interact with as part of their job, on social media.
- Staff must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations, George Abbot School, or the wider community.
- Staff members must be accurate, fair and transparent when creating online web space and social media accounts.
- All School Social media accounts are to be set up by the Communications Officer (PRJ)

4.6 Use of Social Media for Personal Use

- Staff members must not have contact through any personal social media with any student, whether from George Abbot School or any other school, unless the students are family members. In the case of family members staff should use a separate social media account to ensure their personal information cannot be seen by other students their child may be friends with.

- All contact with ex-students must be done through the school email system and official school sites for at least three years after the ex-student has left George Abbot. Staff must use the school email to communicate directly with any ex-student.
- Staff members should avoid having any contact with students' family members through personal social media to reduce the risk of current students having access to the information of staff members through their children who are at school. Any potential or actual communication with current students, other than through school email, should be discussed with the DSL. The DSL will evaluate each scenario in context and formulate a risk assessment if needed.
- Staff members must decline 'friend requests' from students received on personal social media accounts and must not follow or be linked with students at school or ex-students for a minimum of three years.
- Information staff members have access to as part of their employment, including personal information about students and their family members, colleagues and other parties and school corporate information must not be discussed on their personal web space.
- Photographs, videos or any other types of images of students and their families or images depicting staff members wearing school uniforms or clothing with school logos or images identifying sensitive school premises must not be published on personal web space.
- School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- Staff members must not 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 employer itself.
- George Abbot School logos or brand must not be used or published on personal web spaces.
- Staff members must set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy.
- Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information.

4.7 Use of Social Media on Behalf of George Abbot

- Staff members can only use official school platforms (e.g. the school's email system or Teams) for communicating with students or to enable students to communicate with one another. Staff should not engage with any direct messaging of students through any social media accounts.
- All School Social media accounts are to be set up by the Communications Officer (PRJ) only. There must be a strong pedagogical or business reason for creating such accounts. Accounts will not be set up if they could expose the school to unwelcome publicity or cause reputational damage. Official school sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements (this is often set at 13 years which would exclude year 7 & year 8). The ramifications and possibilities of children under the minimum age gaining access to the site must also be considered. The social media account or profile must not encourage anyone under 13 to use social media. 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.
- Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of George Abbot School.
- Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task but involves a considerable time commitment. As such unused sites or accounts should be deleted to ensure they are not neglected creating a potential risk to the school's brand and image.
- All official school social media accounts must be accessible by more than one member of staff and private messaging functionality should not be used except when conversing with other professionals. The social media account must be monitored by a member of the senior leadership team.
- Staff must not publish photographs of children without the written consent of parents/carers, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts.

- Any abuse of school-sanctioned social media (through either staff involvement or a compromised account) should be reported to the DSL or SLT and recorded for safeguarding purposes. Any offending material must be deleted and if necessary, the account removed. Screenshots should be created prior to deletion in order to maintain evidence in cases where breaches of confidentiality, defamation or damage to the reputation of George Abbot School has occurred.
- Any complaint or queries made about or through school social media accounts must be relayed to a member of the senior leadership team immediately, with an acknowledgement of receipt or response made within 5 working days. Any abusive messages or comments must be removed swiftly with sensitivity.
- Photographs or videos of students must only be uploaded after checks have been made to ensure that the student has parental consent for the image to be used. Staff must use professional judgment when using images. Students must be appropriately dressed and not be placed in a situation that would make them open to ridicule. Names must not be used when linking photos to pictures. If a name is mentioned, without a photo, this must be first name only.
- Use of communication apps, such as WhatsApp, must not be used for business or school purposes. Any communication must be conducted on official school platforms such as email or Microsoft Teams.

4.8 Use of Video Functions for School Purposes
Staff must not contact students using any other forum, other than school email, or invite students to join any another forum.

Any inappropriate behaviour or actions by a student or groups of students should be reported to the Head of Department or Inclusion Manager.

In order to avoid allegations, staff must self-refer any inappropriate attention from a student or group of students to the Designated Safeguarding Lead.

4.9 Photographs
Under no circumstances should members of staff use their personal equipment to take images of students at, or on behalf of, the school or display or distribute images of students except as authorised by the school and with appropriate consent. Staff may take images of students on school equipment for school purposes only. Images of students (i.e. for trips, visits, events etc.) must only be stored on the school network in an appropriately named folder.

5. Online bullying
Bullying is "behaviour by an individual or a group, repeated over time that intentionally hurts another individual either physically or emotionally". This can take place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy and Anti-Bullying Policy.)

To help prevent online bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. George Abbot uses worried @ for reporting concerns (which can be accessed from home), students can email relevant staff, are encouraged to speak to their Head of Year of Form Tutor.

George Abbot actively discusses online bullying with students, through Form time discussion, Assemblies and PSHE lessons, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff, governors and volunteers (where appropriate) receive training on online bullying, its impact and ways to support students, as part of safeguarding training.

In relation to a specific incident of online bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained and take action in accordance with Keeping Children Safe in Education (KCSIE) 2024, Working Together to Safeguard Children, Child Protection and Safeguarding Policy, Sharing Nudes and Semi-nudes. The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6. How the school will respond to issues of misuse/ Responding to Online Incidents and Concerns

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and the Student Acceptable Use Agreement**.** The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Any breach of this policy, including misuses the school's ICT systems or the internet may lead to disciplinary action being taken against the staff member/s involved in line with the Trust's Disciplinary and Capability Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

7. How the school complies with changes to statutory guidance.

The Network Team are working in partnership with the Safeguarding Leads (DSL/ DDSLs) to comply with the changes made in Keeping Children Safe in Education (2024) statutory guidance on E- Safety to provide a safe learning environment for all members of the school community.

- The Designated Safeguarding Lead (DSL) takes the lead responsibility for online safety and has appropriate knowledge of the filtering and monitoring system and processes that the school has put in place. The DSL is supported by the Central Safeguarding team; however, the overall responsibility is not delegated.
- The school also has an online safety coordinator who works alongside the DSL.
- The school regularly reviews effective practice of all filtering and monitoring security procedures.
- The Central Safeguarding Team (DSL/ DDSLs) and the Networking Team are responsible for understanding and ensuring effective filtering and monitoring systems that the school has in place.
- Clear guidance and training are provided to the safeguarding teams regularly, identifying roles and responsibilities for members who deliver the effective and efficient monitoring system.
- The Network Team and the Central Safeguarding Team will review and reflect on approaches to online safety, including appropriate filtering and monitoring on school devices and networks, to ensure procedures align with new technological advances in cybercrime.
- All staff members understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring, highlighted in the changes in KCSiE 2025, through regular training and updates.
- School investment in the Securus Full Monitoring Service enables daily monitoring checks of the school community's safe use of the internet.
- Parity is achieved through connecting the Securus Systems with CPOMs to report, record and action concerns. The use of CPOMs enables the identification of risk through analysis of trends within varying cohorts and on an individual basis. Regular reviews will enable better understanding of areas that need further scrutiny with educative approaches to ensure E- Safety.
- The appropriateness of our filtering and monitoring systems are informed in part, by the risk assessment required by the Prevent Duty.
- The Central Safeguarding Team including the SENCo and Mental Health Lead regularly review those who are potentially at greater risk of harm and how often they access the IT system.
- Child-on-child abuse online is dealt with in accordance with the Safeguarding Policy to prevent and respond to any incidents when they occur, even if they take place offsite including sexual harassment.
- The schools recruitment process is transparent and ensures that shortlisted candidates are aware that online searches may be done as part of due diligence checks.
- School provides regular and appropriate parental engagement in online safety, and specific concerns are responded to in line with child protection policies.
- The DSL ensures online safety approaches are regularly reviewed and supported by an annual risk assessment that considers and reflects the specific risks their children face.

George Abbot School Student IT Acceptable Use Agreement

George Abbot has the responsibility of providing you with safe, reliable and useful IT resources that will help you make the most of your learning opportunities. You have a right to these resources, however, with this right comes the following responsibilities:

All online activity will be appropriate to:

- *Ensure the safety and security of the school system.*
- *Ensure respect for all members of our community.*
- *Ensure the safety of all members of our community.*
- *Maintain the reputation of the school.*

School owned, and managed IT devices and connected personal IT devices/networks including phones, consoles, tablets and computers, must not be used for any illegal, obscene, offensive, profit making or commercial purpose or for anything other than school business. The school network is monitored to make it difficult for students to access inappropriate content.

I will take responsibility for my own use of all technology made available to me, making sure I use it safely, responsibly, and legally. In particular, I understand I must:

- Take responsibility for all activity that takes place under my network login. I will not let anyone else use my network login. Keeping my passwords confidential.
- Not install any software on any school owned device without the consent of the Network Manager.
- Not alter any of the settings on school owned devices or attempt to 'hack' into the school network using a web browser, DOS or any other method.
- Report any IT problems/issues to the Network Team immediately.
- Not use or connect any personal equipment such as mobile phones, cameras or other electronic devices to the school IT system or take, publish, live stream or circulate pictures or videos of anyone or live stream.
- Only store schoolwork related files on the network.
- Only use school internet and email systems for school related work and assume responsibility for any sites visited, content viewed or emails received/sent using or on a school device/network.
- Use email/electronic communication responsibly and always be polite and respectful. I will only use email systems and other communication methods that are approved by the school. I will never use IT for bullying or harassing others or in a way that will bring the school into disrepute.
- Inform the Network Team immediately if inappropriate sites are accessed by accident.
- Not access social networking/chat room sites in school and I should never agree to meet people I have met online.
- Not pass on anyone else's contact details without permission.

I understand a breach of this Student IT Acceptable Use Agreement:

- May result in the temporary/permanent loss of access to school devices and IT systems.
- Will result in a sanction in line with the school's behaviour policy.

Remote Learning Agreement

This document is designed to support safe and effective home learning for our students should there be a period of partial or full lockdown for any classes, year groups or the whole school.

Parents/carers are required to sign this agreement so students may participate in interactive virtual teaching and learning with George Abbot teachers. This agreement should be read in conjunction with our Student IT Acceptable Use Agreement which can be found above (www.georgeabbot.surrey.sch.uk/policies). It outlines the parameters all students and parents/carers are expected to adhere to, in order to engage safely in interactive and live learning online with each other and our teachers.

Parents/Carers, we ask you and/or your child:

1. Establish a tidy, suitably resourced working desk or table at home, with access to Wi-Fi, computer or other suitable device and free from unnecessary distractions.
2. Set up a separate online folder for each subject they study.
3. Follow the timetable as set out for any lockdown period.
4. Submit work via the SLE or other platform such as Google Classroom, as requested by the teacher.
5. Complete work during lessons as requested by the teacher.
6. Contact your teachers via email if anything is unclear or you need extra support.
7. Be dressed appropriately for any face-to-face learning in a school polo shirt.
8. Have had a discussion about appropriate behaviour in a remote lesson; treating other students with respect and waiting to be invited to speak so the same standards are maintained remotely as would be in a real classroom.
9. Understand parents/carers and students are not allowed record video or audio, photograph or share any images or recordings from interactive lessons.
10. Understand parents/carers must be aware when our students are engaged in learning with their teacher and therefore this should be in line with the lockdown timetable only.
11. Keep their passwords safe and secure.
12. Understand any deliberate browsing, downloading, uploading or forwarding of material that could be considered offensive or disruptive does not occur in remote learning lessons.
13. Understand when using Zoom/Teams, lessons will be recorded for monitoring and safeguarding purposes. These recordings will only be available to identified staff as directed by Mrs Carriett to support safeguarding and effective teaching and learning for our students.

Students, please agree to this simple agreement:

I understand Zoom/Teams is an extension of the classroom and I should conduct myself as I would in a classroom environment. This includes:

- Taking part in a Zoom/Teams meeting in an environment that is safe, quiet and free from distractions (where a bed is not visible).
- Being on time for the virtual meeting.
- Being dressed appropriately for learning.
- Remaining attentive during sessions.
- Interacting patiently and respectfully with my teachers and peers.
- Not recording, live streaming or photographing each other's online interactions.
- Finishing the session when my teacher instructs me to do so.

If you have any questions/queries with the above, please email network@georgeabbot.surrey.sch.uk

IT Online Learning Support

SLE – Student Learning Environment. Purely for students, where they can access work shared by teachers if they are absent from school. It is set up by subject, and all lesson PowerPoints/resources should be on here. Work can also be submitted for teachers to review etc.
https://georgeabbotschool.sharepoint.com/sites/SLE/SitePages/Home.aspx

Google Classroom – A virtual classroom used by the Computer Science/IT Teams. This can be accessed via the SLE (above), or by logging in via https://classroom.google.com/u/0/h

- **Username:** first four letters of your surname, followed by the first four letters of your first name, followed by a full stop and then the year you joined George Abbot. E.g. John Richards joining in 2021 his log in would be RICHJohn.21, followed by @georgeabbot.surrey.sch.uk
- **Password:** Passwords are set by the Computer Science team.

School Network and Email

- **Username:** first four letters of your surname, followed by the first four letters of your first name, followed by a full stop and then the year you joined George Abbot. E.g. John Richards, who joined in 2021, log in would be RICHJohn.21

- **Password:** Passwords are changed throughout the year but if you forget yours, just email the Network Team (networkhelpdesk@georgeabbot.surrey.sch.uk).
- At school, email can be accessed through the Student Hub.
- At home you can access it by clicking on the email link on the George Abbot homepage. Instructions on how to access the email system can be found by clicking on the logo next to the email link.

Appendix 2: George Abbot Student Acceptable Use Agreement

IT Equipment Loan Policy

By signing this document, you agree to -

- Adhere to the ICT Acceptable Use Policy/Code of Conduct/Data Protection & Information Policy
- Take care of the equipment supplied to you

Please note:

- You must make regular back-ups of your data onto an encrypted USB or OneDrive to avoid loss of data should the equipment need to be restored back to the original settings at any time.

I UNDERSTAND THAT GEORGE ABBOT SCHOOL WILL NOT BE RESPONSIBLE FOR THE LOSS OR MISUSE OF OR DAMAGE TO THIS EQUIPMENT INCLUDING ANY HARDWARE, SOFTWARE OR DATA

This is to confirm that I have received the following:

NAME			
STAFF	☐	**STUDENT**	☐
DESCRIPTION	– Replace Value of £ 250		
Machine Name	GA-		
CONDITION	Good		
Accessories	☐ Headphones ☐ Mouse ☐ Keyboard ☐ Charger with Mains cable Other:		
DATE ISSUED		**RETURN BY**	
SIGNATURE			

Upon return of the device and applicable accessories:

DATE RETURNED	
CONDITION (Agreed with by IT)	
SIGNATURE	

Learning Partners academy trust

Learning Partners Academy Trust
A company limited by guarantee, registered in England and Wales, company number 08303773
Registered office: c/o Guildford County School, Farnham Road, Guildford, Surrey. GU2 4LU