



GUILDFORD HIGH SCHOOL

4-14 USE OF TECHNOLOGY

Contents

POLICY STATEMENT.....	2
THE IT SUPPORT TEAM.....	3
EQUIPMENT.....	3
STRATEGY.....	4
IN THE CURRICULUM.....	5
REMOTE TEACHING.....	6
PUPIL DEVICES.....	6
ARTIFICIAL INTELLIGENCE.....	7
PHOTOGRAPHY.....	8
SOCIAL MEDIA – PROFESSIONAL USE.....	9
SOCIAL MEDIA - PERSONAL USE.....	10
DATA AND GDPR - Technical and organisational measures for keeping data secure.....	11
ONLINE SAFETY.....	12
DIGITAL LIVING.....	13
APPENDIX 1: STAFF IT ACCEPTABLE USE POLICY.....	14
APPENDIX 2: PUPIL ACCEPTABLE USE OF TECHNOLOGY POLICY.....	16
APPENDIX 3 – SOCIAL MEDIA GUIDE.....	19
SUMMARY OF BASIC PRINCIPLES.....	20
APPENDIX 4: PHOTOGRAPHY AND FILM CONSENT FORM.....	27
APPENDIX 5: USING YOUR DEVICE AT HOME POLICY.....	28

POLICY STATEMENT

The use of ICT at Guildford High School is primarily to enhance learning through the use of established and innovative technologies. Our mission is to provide a first-class education to academically able girls. We therefore aim to promote new and exciting technology to make our classrooms even more stimulating environments, and to enhance independent learning.

Guildford High School's aim is to use ICT, where appropriate:

- To enhance the learning experience of our pupils
- To facilitate best teaching practice by teachers, both in the classroom and in their assessment of pupils' progress
- To improve effectiveness, achieve efficiencies and promote best practices in administrative systems.

To support our mission, Guildford High School has a number of policies and procedures in place to guide and support those who use ICT. Both pupils and teachers have access to computer resources, e-learning, Wide Area Network (WAN) that ensure safe, secure and timely access to e-mail, e-learning resources and educational software.

However, we are mindful that technological safeguards go hand-in hand with promotion of best practice, responsible and appropriate usage and so our ICT policy and procedures documents are intended to promote positive outlook and behaviour regarding responsible ICT usage and online safety. These are the responsibility of every member of staff: teaching, administration and support.

This policy applies to all members of our school community, including those in our EYFS setting. The school is committed to ensuring that the application of this policy is non-discriminatory, in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunities Policy.

The governor with responsibility for e-Safety meets annually with the Assistant Head - Teaching and Learning to jointly review the school's approach to e-Safety. Regular contact is also maintained throughout the year.

This policy is reviewed annually, or more often if legislation changes or events require, by the Deputy Head (Academic), in discussion with the Assistant Head - Teaching and Learning, the Network Manager and the Database Manager. The next date for review is September 2026.

All members of staff have to sign the Receipt of Policies form when they join the school, which acknowledges that they have read this policy. Staff are required to read and sign again following substantive policy updates.

This policy should be read in conjunction with:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- UCST disciplinary procedures
- Privacy Notice

- Behaviour and Discipline Policy
- Anti-Bullying Policy
- UCST Clear Desk Policy

This policy contains the following appendices:

[Appendix 1: Staff IT acceptable use policy](#)

[Appendix 2: Pupil acceptable use of technology policy](#)

[Appendix 3: Social media guide](#)

[Appendix 4: Photography and film consent form](#)

[Appendix 5: Using your device at home policy](#)

THE IT SUPPORT TEAM

Name	Position	Location
Charles Baddock	Network Manager	Network Manager Office
Luke Jupp	Assistant Network Manager	ICT 2
Rosana Vilaplana	Database Manager	Harper House (First Floor)
Martin Comfort	IT Systems Administrator	Junior staffroom
Hatty Whitfield	IT and AV Technician Online Safety Lead	ICT 2
Joonas Arola	Technician (Part time)	Harper House (First Floor)

Additionally, there is the AV team:

Name	Position	Location
Conor Brown	AV	Media suite
Charlotte Smith	Multimedia Technician	Media suite

Technical support can be requested by e-mail (ghsitsupport@guildfordhigh.co.uk), by phone or in person. If the request is not urgent, a completion date should be included. IT Support aim to respond to requests for assistance in lessons within ten minutes.

EQUIPMENT

- Each classroom has a a laptop docking station, an interactive whiteboard or touch-screen TV, and an Apple TV.

- There are also ICT rooms, with desktop PCs for each pupil, which can be reserved using the Room Bookings system.
- In the Senior School, all teachers and pupils have an iPad and Apple Pencil. These are leased on a 3-year contract via Albion Computers.
- In the Junior School, all teachers and pupils in years 5-6 have an iPad and Apple Pencil. Pupils in year 3-4 have an iPad.
- School iPads are managed via JAMF.
- The internet filtering within the school site is provided by Securly. Parents are advised to ensure there are appropriate filtering settings on their home network as iPads are only filtered on the school site.

STRATEGY

Technology is not a defining feature of lessons, but rather a tool that is used as and when it will have a positive impact. The use of Apple Pencils to complete appropriate tasks is common, however work involving extended writing is invariably completed on paper. The exception to this is the small number of cases where use of a word processor is the pupil's normal way of working (e.g. where handwriting is challenging due to a physical condition, or where pupils plan to take public examinations using a laptop).

Through INSET training, CPD sessions, staff meetings, electronic communication, the Digital Teaching support site and informal conversations, we aim to equip staff with an understanding of a range of recommended electronic tools and platforms, and to provide potentially effective ideas and strategies. We ask that staff:

- Make their own informed decisions about how and when to incorporate iPads into their lessons.
- Continuously evaluate their use of technology and consider where it can have a positive impact.
- Do not feel compelled to use the devices at every opportunity just because they are there – if a task is better without them, they should definitely not be used.
- Remain open to new ideas and be willing to try new things in their teaching.
- Share good practice via department meetings, informally in the staff room and through the CPD programme.
- Seek help if they would like to achieve something through the use of technology but they are having trouble or they are not sure how.

It is expected and desired that different teachers and different departments will not use the technology to the same extent or in the same ways. It will also be appropriate at times for individual teachers to modify their approach depending on the class or even specific pupils they are teaching. Over the course of a school day, we therefore expect pupils to encounter a variety of teaching styles and activities, some electronic and some more traditional, chosen to suit the teachers, pupils and subject material involved.

IN THE CURRICULUM

There are three electronic tools that all Senior School teachers must use with their classes, both of which can be accessed either online or via an app:

- Teachers.io is used every time a piece of homework is set. The details of the work are entered by the member of staff, and this is visible to pupils through the myHomework app. This system makes the process of setting homework more efficient, minimising the time wasted during lessons, although it is still essential for teachers to explain homework tasks to pupils in person.
- In line with department workflow policies, either OneNote or Showbie is used as the digital folder for every class. Here, digital schoolwork is stored alongside scanned paperwork completed on paper to ensure effective organisation.
- ePraise is used to award house points to pupils throughout the Senior School.

Staff should avoid sharing YouTube links with pupils, as this will lead to suggested content and comments that are outside of our control. Instead, video content can be shared in more controlled environments, such as via ClickView or Microsoft Stream.

Beyond this, is it up to individual teachers to decide how and when to use technology. Some of the key benefits of having it at our disposal include:

- The ability to efficiently share a wide range of resources. At a basic level, this could be the equivalent of having an electronic version of a sheet rather than a printed version, but we can also share videos, weblinks, interactive activities and more. We can provide an organised space in which resources are collated and curated for particular classes, and of course pupils and staff can also find information in an impromptu fashion whenever required.
- Participation. Before having mobile devices in the classroom, if a teacher were to ask a question to a class, usually just one pupil would have the chance to respond during a discussion. With the iPads, there are many ways in which we are able to get responses from every pupil simultaneously and use them to further a discussion.
- Communication and collaboration. Pupils and teachers are able to communicate much more efficiently and collaboration between pupils is made simpler.
- Feedback. Teachers can respond to pupil questions outside of lessons, so that a pupil who is stuck on something does not have to wait until the next lesson to get help. Rich feedback is possible through the use of electronic annotation, pinned text notes, voice notes and video.
- Organisation. The electronic planner and the ability to access textbooks and other resources online mean that pupils do not have to remember to transport such a large variety of items to and from school each day.
- Activities that are not possible without the technology. For example, making a recording of yourself speaking a foreign language, using electronic revision tools to streamline the revision

process, using graphing software in Maths to immediately see the effect of changing a variable, low-stakes automated testing, video analysis in PE/Drama, creation of video presentations etc.

REMOTE TEACHING

For periods of remote teaching, as during Covid-19, the following principles apply:

Senior School:

- All lessons are taught synchronously through scheduled Microsoft Teams calls as per the normal academic timetable. Pupils must join lessons with their microphone muted unless otherwise directed by their teacher.
- For periods of hybrid teaching (when only some pupils/teachers join lessons remotely), pupils/teachers continue to join lessons through Microsoft Teams.
- Through OneNote and Showbie, class workflow continues in the normal manner.
- Through tools such as breakout rooms and together mode in Microsoft Teams, discursive tasks for small groups are encouraged to aid pupils' learning and well-being.
- At the discretion of the teacher, lessons are shortened by 5-10 minutes to allow for longer breaks between lessons.
- Training is given to pupils and teachers by the Assistant Head - Teaching and Learning through email, CPD sessions, 1:1 meetings, and resources on the Digital Teaching and Learning support sites.
- Technical support is provided by IT through the IT support email address (ghsitsupport@guildfordhigh.co.uk).

Junior School:

- In Reception and Year 1, tasks and instructions are emailed to parents each evening to be completed the following day. Parents then email the completed work back to teachers. Each pupil in these two year groups had a weekly one-on-one catch-up call with their teacher. Pupils read aloud to teachers, who were also able to monitor pupils' well-being.
- In Year 2, pupils had synchronous Teams lessons in core subjects and some others, totalling approximately two thirds of their normal timetable.
- In Years 3-6, arrangements are identical to those in the Senior School.

PUPIL DEVICES

Pupils are expected to take care of their school iPads and Apple Pencils:

- All Senior and Junior School pupils should take their iPads and Apple Pencils (if applicable) home with them and bring them to school each day, charged and ready for use.
- iPads must stay in their cases at all times.

- Apple Pencils should be kept in the iPad case when not being used to prevent loss. The loss of an Apple Pencil by a pupil incurs a subsidised chargeable fee for a replacement.
- Pupil iPads must have a name label clearly displayed on the back and Apple Pencils must have a numbered sticker label. These are provided when the devices are first given to the pupil, but replacements can be requested from the IT Support team.
- iPads and Apple Pencils should not be left unattended around the school – they should be with the pupil or in their bag.
- Loss or damage should be reported to the IT Support team as soon as possible.
- iPads must be password protected. Pupils should not allow others to have unsupervised access to their device, and they must not attempt to gain access to devices belonging to other pupils or staff members.
- All sixth form pupils are permitted to bring their own device into school to support their studies and may access the internet through the GHS BYOD network. Following consultation with the Assistant Head - SENDCo and the Assistant Head - Teaching and Learning, pupils in lower year groups who have exam access arrangements, may also be permitted to bring their own device into school for use in lessons or use a Bluetooth keyboard. It is advisable that any device brought into school should be suitably insured.

The apps and settings on pupil iPads are controlled by JAMF, the Mobile Device Management system. Pupils have access to apps that have been automatically sent to them as well as some that we have selected to be available to download via the GHS Hub.

During lessons, iPads should be used as instructed by the teacher. When not in use, it is good practice for the cases to be closed so that the screen is not visible. Information about sanctions for inappropriate use of iPads in lessons can be found in the Behaviour and Discipline policy.

When communicating electronically with staff, pupils should always use their GHS e-mail accounts. Junior School pupils do not have access to a school e-mail account.

iPads must not be used by pupils when they are walking around in school corridors, and they must not be used in Stocks Hall during break or lunchtime.

The school does not take any responsibility for the security of pupils' personal devices. For Years 7 to 11, any mobile phones brought into school must be in lockers between 08:30 16:00. Failure to comply with this rule will be sanctioned with a detention. Sixth Form pupils may keep their mobile phones with them, but they should not be out during lessons. Very few Junior School pupils bring a phone to school, but those who do should give their phone to their teacher at the start of the day.

ARTIFICIAL INTELLIGENCE

The use of Artificial Intelligence (AI) such as Mindjoy (the school preferred AI platform) offers a valuable opportunity to enhance learning, explore new ideas, and engage in meaningful conversations. We will harness the power of AI to enhance education, support students and teachers, and create

inclusive learning environments. Pupils will sign the appropriate use of technology policy (see appendix 2).

The following principles will guide our use of AI:

- **Transparency:** We will be transparent and accountable in our AI decision-making processes.
- **AI accuracy and bias:** When using AI, we will be mindful that AI can be inaccurate and biased. We will be vigilant about identifying biases that derive from the data AI has been trained on or the ethical overlay that humans have added.
- **AI limitations:** While recognising and utilising the power of AI for educational benefits, we will also acknowledge its limitations and seek to combine the best of what AI can do with the creativity, intuition and understanding that only human beings are capable of.
- **Equity and inclusivity:** We will consider using AI to broaden our communities, bridge the digital divide, and create a supportive and inclusive AI culture.
- **Mental Health:** We will be mindful of the potential of AI to impact both positively and negatively on mental health and will teach pupils to use it responsibly.
- **Student Empowerment:** AI should encourage active engagement, independent learning, and the development of skills and dispositions for life. The capacity of AI to stifle independent thinking and creativity and to ‘steal the struggle’ from students is acknowledged and should be avoided.
- **Creative Collaboration:** We should embrace AI's opportunities to work together to be creators, not just content generators.
- **Responsible Innovation:** We will use AI responsibly and thoughtfully, considering the potential benefits and trade-offs associated with AI, such as its impact on our brain development and learning.
- **Shared Learning:** We will share the burden of ongoing research, development, and creating ethical guidelines around new tools with our staff and students. We will create safe spaces to ideate and discuss the risks and opportunities around AI.
- **Data Protection:** No personal data should be used with any open access AI tools. DPIA's are likely required should a staff member wish to use an AI in this way, and this will only be permissible upon discussions with the Assistant Head – Teaching & Learning and Data Protection Officer.

PHOTOGRAPHY

Staff are encouraged to use school devices to take photos and videos of school trips and events. These can be shared publicly via the GHS Trips Twitter account or a departmental account (see *Social Media – professional use*), used in displays around the school, passed on to the Marketing team for use in promotional material, or saved on the Photos drive. Once the material has been saved or shared as necessary, it should be deleted from the device on which it was taken. When taking photos or videos, staff should:

- Only use school devices.

- Be aware of the Do Not Photograph list (a small number of pupils who must not appear in any school photography) – this can be found on the intranet under *Useful Documents*.
- Where possible, avoid focussing on an individual pupil.
- Inform parents before a trip if a particular account (usually @GHSTrips) is going to be used to share photos, videos and other information about it.

With the exception of those on the Do Not Photograph list, all pupils' parents have signed the Photography and Film Consent Form (see Appendix 4), confirming willingness for daughters to appear in photos and videos for GHS purposes. If you wish to share a photo/video externally to a supplier, trip organiser etc. specific permission must be sought from parents of each pupil appearing in the photo/video. Additionally, specific consent is required if images of a pupil are to be used as part of a large advertising campaign or promotional film.

It is accepted that parents may wish to take photos or videos of their daughters at school events. This should be done discreetly, without disturbing performers or other spectators. Where possible, footage should focus only on their own child. Any media containing images of other pupils must not be shared online without the explicit consent of all involved.

Pupils must never film or photograph staff or other pupils without their knowledge, nor should they film or photograph anybody who expresses any unhappiness in being recorded in this way.

Children in the EYFS setting must not be filmed or photographed by any parents or pupils. Cameras must never be used in changing areas or bathroom facilities.

SOCIAL MEDIA – PROFESSIONAL USE

Members of staff may wish to use social media in a professional capacity, for example running a departmental Twitter account or writing an educational blog. Where accounts are publicly visible and the user is identifiable as a member of GHS staff, all content reflects on the school and must remain professional. Members of staff wishing to begin using social media for professional use should read the guidelines (Appendix 3) and seek advice from the Marketing team.

Social media can be extremely effective as a promotional tool, for professional development and for sharing engaging content with pupils. Active school Twitter accounts such as @GuildfordHigh, @GHSTrips, @GHSSeniorSport and @GHSjuniorsport are all good examples of this.

When using a social media account professionally, staff should:

- Use strong passwords.
- Password protect any devices with access to the account so that a third party gaining control of a device could not make posts on their behalf.
- Share the log-in details with the Marketing team.
- Proof-read posts to ensure correct spelling and grammar.

- Be wary of automated location tagging.
- Avoid sharing overtly political content.
- Be aware that sharing inappropriate content (foul language, inappropriate images, racist/sexist/homophobic or otherwise prejudiced content) is likely to result in disciplinary action.
- Avoid using copyrighted photos or written content without permission or crediting the source.
- Be careful to check that any material shared from other sources does not contain inappropriate content (for example, when sharing a link to another site or re-tweeting another account).
- Not follow any pupil accounts, with the exception of those that are set up explicitly for school projects, e.g. a Young Enterprise team.
- Report any concerns, such as hacking, trolling or inappropriate contact from pupils, to the Marketing team and SLT immediately.

When sharing photos and videos of pupils online, staff must follow the guidelines in the *Photography* section above. Additionally:

- The name of a pupil must not appear alongside an image of them (this includes any name badges that may be visible on a pupil's clothing or equipment – if necessary, these must be blurred before the image is shared).
- If the photo is of pupil work, rather than the pupil themselves, the first name of the pupil can be shared.
- All pupils must be dressed appropriately. If they are wearing school uniform, it must be correct.

Before leading a school trip, staff should speak to the Marketing team about the use of the GHS Trips Twitter account.

SOCIAL MEDIA - PERSONAL USE

Where staff use social media in their personal life, it is imperative that the privacy settings are secure so that pupils and parents are not able to access profiles. Dating websites should be used with caution if there is a possibility of crossing paths with pupils. The sharing of inappropriate content online may lead to disciplinary action.

Staff should not make contact with any current pupils on social media. Any contact on social media from current pupils should be ignored and, if necessary, reported to SLT. It is acknowledged that some staff, particularly those with children at the school, may have friends who are, for example, parents of GHS pupils. In these cases, staff may be in contact with relatives of pupils on social media, but they must exercise caution and professional judgement, avoiding any potential conflict of interest. Staff wishing to befriend students who are over 18 and who have left school, perhaps because of a shared extra-curricular interest such as music, should do so with caution. Any content posted on either ex-students' or their own social network may not only compromise their own position but that of any colleagues with whom they are also friends and who may not want their content to be seen by any ex-student.

DATA AND GDPR - Technical and organisational measures for keeping data secure

Staff are educated about the use of data and the UK GDPR regulations via online training, staff meetings and INSET. The Data Protection Leader, in conjunction with the Data Protection team at United Learning Head Office, ensures that all of the digital tools used within the school are UK GDPR compliant and maintains a record of the data held within them. Before any new tools are introduced, they are referred to the Data Protection Lead for assessment, to ensure compliance.

Any device with access to the school network must be password-protected, and passwords must not be shared. Computers and mobile devices with access to sensitive data must be locked when unattended. The use of unencrypted USB drives is not permitted.

Care should be taken when sending potentially sensitive information via e-mail. Staff should check the recipient list carefully, particularly if choosing to 'Reply to All'. Any e-mails received in error should be deleted. When emailing externally to more than one person, staff should always use the blind copy ('bcc') function, especially when contacting parents. When sending personal data, this must be encrypted or password-protected, in line with the UK GDPR requirements, for example by using a OneDrive link. The Data Protection Lead should be informed when there is a need to share data with a third-party organisation, for example when an educational visit is being planned. In this assistance, the Data Protection Lead will coordinate a Data Protection Impact Assessment (DPIA) to help to identify and minimise the data protection risks of the trip or project.

Data must not be transferred outside of the United Learning/Guildford High School systems except via school e-mail or the use of encrypted media. Personal cloud storage and personal e-mail accounts must not be used for this purpose.

To improve the security and confidentiality of information, the school has adopted the United Learning Clear Desk/Screen Policy for classrooms, shared work areas and computers. For more details, please check the [Clear Desk Policy](#)

Under GDPR there is a requirement for organisations to:

- Respond to subject access requests (SARs) without delay and within one month of receipt of the request.
- Report to the Information Commissioner's Office a notifiable personal data breach within 72 hours after having become aware.

Individuals have the right to access and receive a copy of all of their personal data that the school holds, and other supplementary information. SARs can be made verbally or in writing, including via social media. A third party can also make a SAR on behalf of another person.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In case of being aware of a data breach, inform the IT team immediately to contain it. Responses to some of the more common causes of data breach might include:

- Lost or stolen devices: IT can wipe the device remotely to prevent unauthorised access.
- Data incorrectly shared, personal data deleted by mistake, email or personal data sent to the wrong person: IT will advise on response and solutions.
- Account being compromised e.g. via a phishing email or inadvertent disclosure of password: IT can change password
- A security incident like a targeted attacks by cybercriminals: IT can investigate and escalate to Head Office if necessary.

The Data Protection Lead will need to gather the following information to determine the level of risk involved:

- When did the incident happen?
- When was the incident discovered?
- Short description of incident.
- What personal data was included in the breach, indicating if any special category data was included (religious, health, racial or ethnic, etc.)?
- How many individuals are affected?
- Has the data been recovered and what steps have been taken / will be taken to recover the data?
- Are the affected people aware?

The school keeps a record of any personal data breaches, SARs, Third Party requests, data protection impact assessments and data processing activities in the [Education Information Portal](#)

ONLINE SAFETY

Through the ASPIRE programme, pupils address online safety issues such as cyberbullying, safe and responsible use of the internet (including the risk of online grooming and/or radicalisation), and sexting. Similarly, online safety issues are covered with staff through the INSET programme, staff meetings.

Within school, internet use by staff and pupils on PCs and iPads is filtered and monitored using Securly. Any inappropriate activity is flagged and a daily report is sent to the Deputy Head Pastoral and the Junior School Deputy Head, who follow up on any suspicious behaviour as appropriate. The Head of receives a weekly report. Staff and pupil iPads are also monitored and controlled via the JAMF mobile device management system. For pupils in Year 11 and below, use of the App Store is restricted and pupils are only able to download apps that have been specifically authorised by the IT team or the Assistant Head - Teaching and Learning. The Senior Leadership Team, in conjunction with the IT team, reserve the right to inspect any staff or pupil iPads at any time if they have reason to suspect that they have been used inappropriately. Use of the internet and digital devices within school may be restricted for any staff or pupils if it is suspected that they have been misused. Any suspected illegal activity will be reported to the police for investigation.

Together with the rest of the IT team, the Network Manager makes sure that the ICT infrastructure with the school is robust and secure, to minimise the risk from misuse, malicious attacks or viruses. All

PCs are protected by anti-virus software. Periodic phishing tests are carried out, overseen by the Network Manager. The Network Manager is also responsible for authorising and controlling access to the school network and to WiFi within school, and for ensuring that passwords for access are secure. When considering the introduction of any new digital tool, and when new features are added to existing tools, the IT team and the Assistant Head - Teaching and Learning assess any potential risks involved.

Staff and pupils are not permitted to install software onto school PCs. Personal laptops are not to be connected to the school network via ethernet and must only be connected to the WiFi via GHS_WiFi. Staff must be wary of opening e-mail attachments from unknown sources and they should not download executable files from the internet. After using a PC, staff must log off, but they should not shut it down completely, as this prevents necessary updates from being downloaded overnight. If leaving a PC temporarily, staff must lock their workstation (press Ctrl-Alt-Delete and choose 'Lock').

Pupils in Year 11 and below who bring a mobile phone into school must keep it in their locker throughout the school day. As such, they are not able to access the internet via 3G/4G within school.

DIGITAL LIVING

All staff and pupils are encouraged to find a healthy balance in their use of technology.

Recommendations are outlined to staff (through the INSET programme and the Digital Teaching support site), to pupils (through the ASPIRE programme and the Digital Learning support site) and to parents (at Reception Evenings, parental pastoral events and the parent section of the Digital Learning support site accessible from the parent portal), including guidance on how to avoid being distracted by notifications, on being considerate in the use of messaging and e-mail, and on managing the use of digital devices at home. For example, it is suggested that:

- Mobile phones and iPads should not be kept in pupils' bedrooms overnight.
- Notifications should be turned off (e.g. using Do Not Disturb feature) when trying to focus on a piece of work.
- Parents should model the expected behaviour with their use of technology and aim to maintain a regular dialogue with their children about it.
- Where possible, use of technology at home should take place in a shared space rather than in a pupil's bedroom.
- Devices should be used sparingly at break and during lunch.

APPENDIX 1: STAFF IT ACCEPTABLE USE POLICY

1. You must read and sign this policy before you can be allowed to use the internet, email or school systems at school.
2. You will keep any personal data secure, in line with your obligations under the UK GDPR and any other applicable data protection legislation.
3. You must agree to the school viewing, with just reason and without notice any emails you send or receive, material you store on the school's computers or your GHS iPad, or logs of websites you have visited.
4. You must only access those services you have been given permission to use.
5. You may bring your own device into school, and you will be able to access the internet via school BYOD WiFi, but not the school network. You must not save any documents of a sensitive nature onto your personal laptop.
6. To maintain a secure and professional environment, all school-related business must be conducted exclusively through your official Guildford High School account. Unauthorised use of personal accounts for school business is prohibited and may result in disciplinary action.
7. You will not transfer United Learning/Guildford High School data outside of the organisation's systems. Office 365 is the only acceptable way of accessing your files remotely. On no account will sensitive or personal data be transferred using any other platform or physical devices (including USBs). Any personal data shared or transferred outside the organisation should always be sent encrypted and marked Confidential. Please speak to IT department for help with this.
8. You will not attempt to remove any of the security measures put in place by Guildford High School to ensure the integrity of its services, the security of its data or the appropriateness of employee activity.
9. You must not leave logged on computers unattended anywhere in the school premises.
10. Any communication from a Guildford High School related account (email, social media) or account which identifies you as belonging to Guildford High School will be appropriate in tone and content.
11. You will exercise caution when sending information via email to ensure that it is addressed to the correct recipient(s) and is the correct information (particularly when attaching documents). Personal data (that by which an individual could be identified) must not be transferred to other recipients unless encrypted or password protected, in line with the requirements of the Data Protection Act.
12. You must not access the internet or email for inappropriate purposes using the school network. The Senior Leadership Team reserves the right to monitor your use of the internet if it has reasonable grounds to believe that you are not using it appropriately. This includes use of the internet on the school network for 'social' reasons e.g. use of Facebook, Twitter/X.
13. The work/activity on the internet and email must be directly related to your school work. You will not use school resources to operate your own business.
14. You must not give your password or login name to anyone. If using a mobile device like your phone or GHS iPad to access your school e-mail or other sensitive information, you must put a passcode on your device for security reasons.
15. Do not download, use or upload or send by email any material which is copyright.
16. Staff should not use personal devices to take pictures of children either in school or on trips without first seeking verbal consent from pupils to do so. Those using personal devices should ensure that any pictures of children are transferred to the school network as soon as possible and then deleted from the device, and any other location the images may have been synchronized to, such as iCloud, local PC or other online storage area. Staff may use their GHS iPad to take photographs or videos of pupils for educational or school marketing purposes.

17. Do not view, upload or download or send by email any material which is likely to be unsuitable for children or schools. This applies to any material of violence, racism, or inappropriate sexual content. If you are not sure about this, or any content with which you come into contact, you must first check with your line manager or a member of SLT. If you accidentally access any such materials, you should inform the Network Manager immediately.
18. The use of offensive language and behaviour online that may bring Guildford High School or United Learning into disrepute is prohibited. This includes email and social media.
19. If you wish to contact a pupil, you should do so via school email and ensure that the tone and content of all communication with pupils is professional.
20. You must ensure that any AI technology is used in a manner that strictly adheres to data privacy law (UK GDPR). Avoid uploading or sharing personal information within the AI tool. Copilot is the preferred AI technology for ensuring the school's data privacy.

Penalties for misuse of computer systems or breach of UK GDPR obligations will depend on the nature and seriousness of the offence. Disciplinary action may be taken against employees who contravene this policy. The school, for various legitimate business practices, may need to monitor the use of email and internet access from time to time for the following reasons:

1. To establish the existence of facts (e.g. the details of an agreement made);
2. To monitor for quality control and staff training purposes;
3. To prevent or detect crime;
4. To investigate or detect unauthorised use of the school's telecommunication system (including email and internet);
5. To intercept communications for operational purposes such as protecting against viruses and to prevent incorrect distribution; and
6. To gain access to routine business communications (e.g. checking email) when staff are on holiday or sick leave.

The school may monitor without notice external and internal email and internet usage including length of use, sites visited and has the right if it wishes to have access any matter sent or received by the user. The school may monitor and assess files to ensure compliance with policy and for the reasons set out above and, in particular, to prevent the use of computer facilities for discriminatory purposes or harassment, and/or the commission of a criminal offence. Should an employee have their access to the internet and email withdrawn, with or without notice, and wish to appeal against this decision, this should be done via United Learning's grievance procedure.

Name:..... Signature:.....

Job Title:

Date:

APPENDIX 2: PUPIL ACCEPTABLE USE OF TECHNOLOGY POLICY

This agreement outlines the acceptable use of technology and AI tools at Guildford High School, detailing the rules and guidelines for using technology resources provided by the school. It covers the use of the internet, email, school-provided devices, and AI tools. All pupils must read and sign this agreement before using these resources.

General Technology Use

- **Internet and Email:** Your activity on the internet and email must be directly related to your schoolwork. Access to social media websites is not allowed on your learning devices.
- **Device Use:** You must not use the internet or email for inappropriate purposes. You should only be using your iPad and Apple Pencil as directed by your teachers in lessons and for your academic work. Sixth Formers may bring a laptop but will only have internet access via school WiFi.
- **Privacy and Monitoring:** The school reserves the right to view any emails, stored material on the school computers, network and iPads, and logs of websites visited with just reason and without notice.
- **Password Security:** Do not share your passwords or login information with anyone. Your password must conform to school guidelines.
- **Photography and Filming:** Do not take pictures or record film of any pupils or staff without permission. Consideration should be given to the appropriateness of uploading pictures or films to social media and, if requested by the subject of the images/film, the files should be removed from all social media platforms.
- **Inappropriate Content:** Do not view, upload, download, or distribute any material unsuitable for children or schools. This includes unkind, violent, dangerous, racist, or inappropriate sexual content. This applies to both school-owned devices and personal devices. If you are unsure about this, you must ask a teacher.
- **Respect and Conduct:** Be polite and do not use strong language, swear, or behave aggressively. Appreciate that others may have views that differ from your own. Cyber-bullying is a serious offence and could result in exclusion or expulsion, with possible police involvement based on severity and risk of harm.
- **Hacking:** Attempts to hack into another user's account or device is not permitted and will be taken very seriously.
- **Device Care:** Follow guidelines for the safe storage and appropriate use of your iPad and Apple Pencil. Wilful or malicious damage will not be covered by insurance. Your iPad must remain in its case at all times.
- **Reporting Issues:** Immediately report any inappropriate or harmful content (such as cyberbullying, inappropriate websites or harmful messages) to a teacher or trusted adult.
- **Mobile Phones** The use of mobile phones by pupils before the Sixth Form is prohibited anywhere in school during the school day (8.30am to 4.00 pm) unless directed by a teacher.

AI Tools Use

General Use: GHS uses the AI platform, Mindjoy for academic purposes. You should not use another AI for academic work, unless specified by your teacher. You may use generative AI tools to generate content (text, video, art and audio) for homework, activities in lessons subject to the conditions and limitations described below.

- **Restrictions:** Do not use AI tools where a teacher has explicitly stated they are off-limits or for tasks designed to be completed without AI i.e. tasks that are expected to be completed offline or in a monitored environment.
- **Coursework:** Use of AI tools in non-examined assessments (NEAs) is subject to JCQ regulations. Seek your teacher's advice and ensure proper citation of AI-generated content.
- **Verification:** Check and verify AI-generated ideas and answers against reputable sources. You are responsible for any inaccurate, biased, offensive, or unethical content submitted. If you are in doubt, ask your teacher.
- **Acknowledgment:** Indicate what part of the assignment was created by AI and what was created by you. You should include which platform you used, website and date. You should also save a log of the prompts and responses, should your teacher wish to see more information.

For example: Mindjoy (<https://beta.mindjoy.com> & name of classroom and tutor),
08/09/2025

- **Plagiarism** Submitting AI-generated work as your own constitutes plagiarism. We reserve the right to use various tools to check for plagiarism and our academic judgment to identify inappropriate use of AI.

Consequences of Misuse

- **Technology Misuse:** Breaches may result in a ban on internet facilities, a letter to parents/guardians, sanctions, exclusion, or other actions decided by the Head and Governors of the school.
- **AI Misuse:** Academic AI misconduct will be reported to the Assistant Head – Teaching & Learning who will address these in accordance with the school's behaviour policy; this may result in your AI privileges being revoked, and/or other sanctions including a reduction or removal of marks.
- **Public Examination Qualifications** Inappropriate use of AI during public examinations or in the creation of coursework is considered malpractice and may lead to disqualification.

If you do not understand any part of this policy, you must ask a teacher.

Agreement

I have read and understood the Acceptable Use of Technology and AI Policy for Pupils.

Pupil Name: _____ Signature: _____

Date: _____

I agree to sign this form on behalf of my child who is below the age of 13 and will ensure they are fully informed about this agreement and what is expected of them.

Parent/Guardian

Name: _____ Signature: _____

Date: _____

APPENDIX 3 – SOCIAL MEDIA GUIDE

WHAT SOCIAL MEDIA MEANS TO US

Countless conversations take place online about schools every day; we want our staff to join those conversations, represent Guildford High School and share the vibrant, supportive and empathetic community that is GHS.

We recognise the importance and benefits of communicating through social media; it is a powerful vehicle through which the school may disseminate relevant news to the school community, listen to voices and perceptions about the school and connect with our audiences online.

These guidelines should guide your participation in social media, both personally as well as when you are acting in an official capacity on behalf of the school. It is critical we always remember who we are – a provider of first-class education, in a caring and vibrant environment, for academically able and characterful girls from age four to eighteen – and what our school’s role is in the social media community – to reach out to girls, and their families, that share our commitment to developing the talents, confidence, resilience and desire to succeed.

The guidelines apply to all members of staff, including those working in our EYFS setting and are reviewed annually by the Marketing Department. It is next due for review in November 2021. The guidelines include:

1. Summary of basic principles
2. Getting started
3. Posting content
4. Maintaining your account
5. Personal use of social media: our expectations

Have fun, but be smart. Use sound judgment and common sense, adhere to the school’s values, and ensure you have read these guidelines in conjunction with:

- Staff-Student Relationships annual letter
- Child Protection policy
- Use of Technology policy

Thanks,

Guildford High School Marketing Department

SUMMARY OF BASIC PRINCIPLES

Social media offers new ways to engage with parents, colleagues and alumnae; this can help build stronger, more successful relationships and contribute immensely to advancing the school's reputation and interests if used properly. If you participate in social media on behalf of Guildford High School, we expect you to follow these basic principles:

- Don't engage without a clear plan, strategy, goals, and line of responsibility
- Be responsible for continuous monitoring, maintenance, and timely response
- Add value with unique, strategic information and commentary about Guildford High School
- Be transparent and avoid misrepresentation
- Write about what you know and stick to your area of expertise when commenting
- Post meaningful, respectful comments — no spam or off-topic or unprofessional remarks
- Always pause and think before posting, and consult with your Head of Department or Marketing Department if unsure
- If you make a mistake, admit it — and be upfront and quick with your correction
- Respect confidentiality of all participants and never disclose student information
- Give credit to sources of written content, images and ideas you reference or use
- Handle negative comments and developments quickly, professionally and strategically
- Always use proper grammar and write accessibly following school style
- Know and follow the school's policies on computing, information, conduct and technology

GETTING STARTED

- Don't engage without a clear plan, strategy, goals, and line of responsibility
 - Creating a social media account requires approval of the Marketing Department. If you would like to set one up, first identify a manager for the social media account.
 - It is important to have at least one dedicated staff member whose job responsibilities include overseeing the day-to-day operation of the account, so that the account does not become inactive or inaccessible.
 - This individual should also identify a back-up staff member with account access.
 - Once a manager is established, but before the account has been created, contact the Marketing Department to:
- Clarify lines of responsibility
 - The individual's role in managing the social media account and who the proposed back-up staff member is
- Confirm which social media platform you want to use

- Which social media platform would you like to use? Approved platforms for our school are Pinterest, Facebook and Twitter
- Briefly explain the purpose of the account
 - Determine your goals and outcomes prior to launching your social media program. Be sure that your program goals support the school's mission, vision and values, as well as those of your department. Be clear how much time you have to devote to social media and realistic about the commitment required. Understand that in some cases, a social media presence is not ideal, and your needs may be better served by collaborating with the main official Guildford High School social media communities or internal platforms
- Set up your account according to Guildford High School guidelines
 - It is important your social media account is set up correctly according to the Guildford High School guidelines, to remain consistent with other departmental accounts and complement the *school's main official Guildford High School accounts*.
 - Once you have approval from the Marketing Department to create your account, they will work with you to:
- Choose a dedicated email address when registering your account
 - It is important not to register with your personal school email address in order to future proof the account in case you leave Guildford High School.
 - The IT Department can create specific email addresses for the purposes of registering for social media e.g. marketing@guildfordhigh.co.uk, biology@guildfordhigh.co.uk
- Creating a strong password
 - Please ensure that your passwords are strong and not easily guessable.
 - Devices which have access to public social media sites should be password protected to ensure third parties cannot send inappropriate messages/posts on your behalf.
 - Any incidents of 'hacking' into your account (and the potential risk for inappropriate posts) or of 'trolling' should be reported to SLT.
 - You must never give anyone your password other than the Marketing Department and your back-up member of staff
- Create an appropriate and consistent username
 - If you have ever seen Twitter or read about it, you have probably seen names that start with the "@" symbol (@GuildfordHigh). These are Twitter usernames.
 - Equally on Facebook, accounts also have a username with the "@" symbol alongside a URL (www.facebook.com/guildfordhigh). Your username is how people will mention you and message you; if someone wanted to tweet/message you or mention you in a post, they would simply include your username in the content of the tweet/message.
 - That would initiate a notification and bring the tweet/message to your attention.

- There is a consistent username set-up that the Marketing Department will aim to follow if available e.g. @GHSBiology, @GHSSport
- Sign the appropriate ‘Account Agreements’
 - Social media services typically require the user to accept ‘Terms of Service’ or other contractual terms and conditions, which are referred to here as the “Account Agreement.”
 - Account agreements are legally binding contracts. They should only be entered into – whether by “clicking through” or other means – by someone authorised to sign contracts of this sort for your department
- Upload the correct branding and profile information
 - Your profile is the page that people see when they click on your username. You should take time to update all of these areas as soon as possible.
 - When people see profiles that are missing information, they tend to assume that the page is not active. You do not want to create that perception of your account, which should be representing the lively and buzzy atmosphere of Guildford High School. The Marketing Department will help you to:
 - Select a strong profile picture
 - Pick a cover photo
 - Complete your description/bio

POSTING CONTENT

- Staff/student contact
 - Please encourage students to follow your department accounts (rather than individual accounts) but remind them about their expected behaviour, which they have agreed to in the Student Acceptable Use of Technology Policy document, and the consequences if they don’t adhere to the rules.
 - Should a pupil attempt to engage with you online in an inappropriate manner, please follow these steps:
 - Do not reply or engage in the conversation
 - Take a screenshot of the incident as a record
 - Report the matter to the Marketing Department and SLT immediately who will decide what action needs to take place

Staff should not follow individual student accounts under any circumstances. However, staff are allowed to follow accounts for school projects such as Young Enterprise, Fashion Show and so on. Staff should not contact pupils directly via social media - all communications with girls must be done through the official channel which is school email. Staff should not engage with online or ‘befriend’ on social media current pupils at the school or former pupils under the age of 18. Staff wishing to befriend students who are over 18 and who have left school, perhaps because of a shared extra-curricular

interest such as music, should do so with caution. Any content posted on either ex-students' or their own social network may not only compromise their own position but that of any colleagues with whom they are also friends and who may not want their content to be seen by any ex-student.

- Respect proprietary content and student information
 - When posting content, it is important to review the information you wish to publish and ensure that you have followed the below:
 - Credit the source
 - Do not use copyrighted photos or written content without properly crediting the source or gaining permission from the source prior to use. Remember, written work is not the only proprietary concern; people's images and comments also require permission to use. Do not "tag" people in photos on public social networks.
 - NB. Any resources which GHS staff create for pupils at GHS remain the intellectual property of the school.
 - Turn off your location settings
 - *Please ensure that your location settings are off so you are not broadcasting your location or that of any girls you mention.*
 - *In addition, some devices may attach the location the photo was taken and so when posted to Twitter, this may still show. Please ensure that you have turned this setting off on your device.*

- Adhere to the school's photography/video guidelines
 - When posting photos, staff must adhere to the photography/video guidelines overleaf, taking into account what they are photographing, girls who must not be photographed, the correct way of labelling the photo and so on.
 - Check the naming: Do not include the full names of any of the girls who are featured in a photograph or disclose the form group they are in - first names are ok. Posts that do not contain a photograph can include full names of girls, but please do not disclose their form group.
 - Review the 'Do Not Photograph' list: Make sure that you are aware of which students are on the 'Do Not Photograph' list and ensure that they do not feature in any photographs you take and wish to post. This list is available on iSAMS and on Useful Documents on the Staff Intranet. Please be mindful of the girls that are not allowed to be in photographs and be sensible towards them when you are taking the photo. It may mean you need to orchestrate the photo sometimes, but that is better than taking a photo you are unable to use, or posting a photo of someone who has not given their permission. If you wish to post a photo of a colleague, it is advisable to get their permission first and clearly explain the context in which the photo is to be used.
 - Look at the content of your photo: Try not to take photos of the girls individually - group shots are better for posting online and mean that the focus is not on one girl in particular. Please make sure that they are appropriately dressed and that, if they are wearing uniform, it is present and correct. Please also use your common sense with

regards to the appropriateness of the photo and think before you post. Please note that any visible name badges must also be blurred.

- Follow Guildford High editorial and brand style
 - The school expects departments and individuals using social media on its behalf to abide by official school standards for branding, graphics and written communications as set forth in the school's *Brand Guidelines*.
 - This includes using standardised account-naming conventions and preapproved graphic templates for cover photos and profile images.
 - Always use proper grammar and write accessibly. Talk to your readers as you would talk to real people in professional situations, without overly pedantic or "composed" language. Do not be afraid to bring in your own personality when appropriate. Avoid any images, graphics, slang or words that may not reflect well upon the school. Draft posts in a program that can detect spelling and grammar errors, and proofread before you post. What you write and publish — including the way in which you name and graphically brand or customise your social media site or account — can have a profound effect on external perceptions of Guildford High School.

MAINTAINING YOUR ACCOUNT

- Listen, monitor and assess continuously to assure constructive engagement
 - Methodical monitoring and assessment, together with active management, is a requirement for engaging in social media successfully and productively on behalf of Guildford High School.
 - Use online monitoring tools to listen and understand your community. Have a plan to monitor what is being said and be responsible for doing so regularly. Check with your site regularly to read comments and respond in a timely manner.
 - Set up automated feeds using search tools such as Google Alerts to notify you of new activity. Keep an eye on followers, know your community and block inappropriate profiles or users who create an inhospitable environment.
 - Also understand that negative comments, criticism or feedback about your program are inevitable aspects of social media. In dealing with such comments, remain detached, refer to the Marketing Department for guidance and respond professionally when appropriate. Any issue of concern (e.g. suicide, threats, violence, etc...) should be reported immediately to the Guildford High School SLT.
- Actively maintain social media accounts and community engagement
 - The school expects all staff engaging in social media on its behalf to ensure that content is kept current, posts are made consistently, and responses are timely.
 - Social media sites with no activity for 90 days or more should be deactivated.
 - Be timely, and treat social media as a real-time conversation in which participants expect information to be distributed quickly.

- Non-activity reflects upon the school just as poorly as negative behaviour. But do not "spam" users or post for the sake of posting. People appreciate the opportunity to give their opinion, so consider content that is open-ended and invites response. Broaden the conversation by citing others who are writing about the same topic. Allow your content to be shared or syndicated, as sharing builds credibility and community and also increases followers. The value of your social media program grows as members contribute.
- "Liking" or "following" sites or feeds should reflect the opinions of Guildford High School.
- Refrain from "liking" or "following" sites or feeds for personal interest or communication. When sharing information from other users via links or "retweeting," make sure that the information is relevant to the audience.
- Adhere to standards of professional conduct at all times
 - Understand that perception is reality. In online social networks, the lines between public and private, personal and professional are blurred.
 - By identifying yourself as a Guildford High School employee, you are creating perceptions about your expertise and about Guildford High School.
 - Ensure that all content associated with you is consistent with your work and with Guildford High School's values and standards. Understand that personal profiles can be linked to and associated with communities you manage professionally.
 - Be a leader and set a positive tone. There can be a fine line between healthy debate and incendiary reaction. You do not need to respond to every criticism or challenge. Frame your comments and posts to invite differing points of view without inflaming others. You are representing Guildford High School; be careful and considerate when discussing sensitive issues, and be cognisant of the potential implications of your comments for the school's reputation.
 - When disagreeing with others' opinions, keep it appropriate and polite. If a user is leaving inflammatory remarks, use your best judgment to defuse the situation. If you cannot help in a meaningful way, recognise that sometimes not responding is the best course of action. If you make a mistake, admit it. Be upfront and quick with your correction.
 - Remember, your mistake will be associated with the school. If you are posting to a blog, you may choose to modify an earlier post — just make it clear that you have done so. Discuss any social media engagement issues, questions, and concerns not covered by these guidelines with the Marketing Department.
 - Don't publish if you can't publish with confidence. If you are about to publish something that makes you even slightly uncomfortable, take the time to review these standards before sending, and think about how they apply to and govern your post. Ultimately, you are responsible and accountable for what you publish on behalf of the school and the consequences thereof.

- Staff should avoid making overtly political statements on their accounts, and any posts of a racist, sexist, homophobic or otherwise prejudiced nature (or sharing of others posts where these are not clearly condemned) will be subject to disciplinary action.

PERSONAL USE OF SOCIAL MEDIA: OUR EXPECTATIONS

- Whether you are an authorised school spokesperson or not, when you're talking about our school, the girls or departments on your personal social networks, keep in mind that:
 - a. Our school's ICT Acceptable Use Policy and other policies still apply
 - b. You are responsible for your actions. We encourage you to get online and have fun, but use sound judgment and common sense
 - c. You are an important ambassador for our school, and you're encouraged to promote it as long as you make sure you disclose that you are affiliated with the school. How you disclose can depend on the platform, but the disclosure should be clear and in proximity to the message itself
 - d. When you see posts or commentary on topics that require subject matter expertise, such as other departments, UK GDPR, the school's performance, or the school's financial performance, avoid the temptation to respond to these directly unless you respond with approved messaging the school has prepared for those topics. When in doubt, contact the Marketing Department
 - e. Be conscientious when mixing your business and personal lives; be sure to know the school's policies regarding personal use of social media at work or on school devices
 - f. On accounts used for professional purposes, staff should take great care when posting pictures of themselves. If they do so, it must be for an educational reason, or simply to identify their page. Staff should not be posting pictures taken for social reasons nor should they be posting content which is not related to their job as employees of GHS
 - g. Ensure that your privacy settings are secure so that students are not able to access your profile, or those that you are friends with
 - h. Please note that it might be a good idea to cleanse your friend list from time to time

If you have any queries or concerns at all, please speak with the Marketing Department or a member of SLT immediately, or if you would like help with your privacy settings, please ask the Marketing or IT Department for assistance.

APPENDIX 4: PHOTOGRAPHY AND FILM CONSENT FORM

As part of running the school we will use photos of our pupils in our electronic systems, in classroom displays and from time to time photos and film may be taken as part of a lesson or project.

From time to time UCST or the school may use pupil photos and films for marketing and publicity purposes. This includes on the school and UCST's website, social media, promotional and advertising materials (including prospectus and newsletters) and for external news providers (printed and online).

We will only use photos or films of your child for such purposes if you have completed this form. Where the school may want to include your daughter as part of a large advertising campaign or promotional film, we would always contact you first to ensure you are happy with this.

I hereby consent to the school and UCST using photos and films of my child for purposes described above:

_____ (insert pupil name)

Signed: _____

Print name: _____

Relation to pupil: _____

Date: _____

You may withdraw your consent at any time. If you wish to do so, please contact us at marketing@guildfordhigh.co.uk. On receipt of such a notification we will remove any images from our websites etc. Please note that if you have consented to the use of images and they appear in the school prospectus or other printed material, we will not be able to remove these images from any documents that have already been printed.

For further information or any questions you may have, please contact us on the details provided below.

The data controller for personal information held by Guildford High School is United Church Schools Trust (UCST). UCST is registered with the Information Commissioner's Office (ICO). The registration number is **Z533407X**.

APPENDIX 5: USING YOUR DEVICE AT HOME POLICY

In case of whole or partial school closure, staff may choose to use their own device in order to work, in preference to their school iPad.

To protect the information on your computer you must:

1. use a log-on that is not shared with anyone else at home;
2. use a complex password and up-to-date anti-virus software.
3. use an up to date, supported Operating System and ensure the latest patches are installed;
4. ensure it is set to auto-lock after a set period of idleness.

All of Guildford High School's staff and pupils can download and install the full Office suite on up to 5 home computers for free. You can do so by signing in to Office.com with you username@guildfordhigh.co.uk and school password.

Important considerations:

- Install both Office
- Once Office has installed, you will need to sign into the individual apps using your school email address and password
- Do not sign in/ activate OneDrive – this is important for data protection reasons.

To avoid inadvertently creating personal data on your computer:

1. email should only be accessed through the browser-based version of Outlook: <https://outlook.office.com>
2. if you receive an email with an attachment, it should be viewed/ worked on in the browser version of Word/ Excel. If it contains no personal data (if it's a teaching resource, for example) then that's fine to be opened in the full version of Word/ Excel if you prefer to. If it contains personal data (e.g. a list of pupil assessment scores) then it is not to be opened in the full desktop application. The reason for this is that using the installed application to open documents creates a copy of them on your computer, which would amount to a breach of GDPR if it ever got stolen/ sold/ accessed by others, etc.

Please talk to the IT Team they will be able to advice you if your device complies with the minimum safety requirement necessary to work securely.

For further information on ensuring online safety when remote teaching, please see appendix 6 of Child Protection and Safeguarding policy and the paragraph entitled 'Children and online safety away from school'.