ICT POLICY (205)
Including EYFS

1. Data Protection Act and GDPR regulations

Please note that all school data is confidential and therefore should be handled with a clear awareness of the Data Protection Act and GDPR regulations (see GDST GDPR Policy and Privacy Statement). A reminder of the key points to remember in association with the GDPR regulations are attached as appendix A. Professionalism and discretion are called for at all times.

2. ICT Code of Conduct

In addition to this document, all staff should make themselves familiar with the ICT Security Code (Appendix B) and the Staff ICT Acceptable Use Agreement [link to GDST Hub] which is given to all new staff upon appointment and which is also available to read on the GDST Hub (for details on how to access the GDST Hub, see below).

Pupils are expected to abide by the "Secondary Pupil Acceptable Use Agreement/eSafety Rules" [see Appendix C]. The content of the ICT code of conduct is discussed with pupils when they join the school and it is reinforced regularly, with annual signing at the start of each academic year.

Throughout the setting, all persons in the EYFS are required to adhere to the above ICT Acceptable Use Agreement on the use of cameras, mobile phones or other digital recording devices; that is, that personal digital recording devices must not be used for talking, editing or transferring images or videos of pupils.

3. Laptops/iPads

The GDST has provided teaching staff at Sutton High School with the use of a laptop or iPad to support teaching and administrative tasks. Staff may recharge the laptop at a convenient place where there is an electrical supply and may store the laptop securely in a department area.

Laptops and iPads are for school use and are the responsibility of the staff to whom they have been allocated. They should be stored securely when not in use. All school data should be stored on the network on the individuals' OneDrive/SharePoint folders as this is backed up regularly. If staff have important files stored on the school laptop, it is their responsibility to make regular backups. The ICT department will not be responsible for any data that is lost on the laptop due to hardware failure, theft or corruption.

All students in Years 4-6 have a one-to-one device and all girls in Years 7-13 are part of the BYOD Scheme, bringing their own device to connect with the school's secure Wi-Fi.

4. ICT Rooms

Senior School has ICT suites in the locations shown below. Classes are timetabled in these rooms but staff are encouraged to make use of the free slots to support teaching and learning. ICT Rooms can be booked using the Room Booking System.

Room	No of PCs	Staff computer	Projection
305	24 desktops	Desktop or use own laptop	Large Screen TV
307	24 desktops	Desktop or use own laptop	Large Screen TV
D11/D21 (Music)	30 Macs	Use own laptop	Large Screen TV
LRC	24 desktops	Use own laptop	Large Screen TV
Discovery Zone (Prep)	22 fixed laptops	Desktop or Use own laptop	IWB

5. ICT Support

The ICT Operations Manager is Les Howlett. There is also a Senior Technician – Keith McPherson, and a Technician – Ben O'Keefe, who provide further ICT support. Their office is located on the Lower Ground Floor of the main building. The team are available from 7:30am until 5.00pm daily during term time.

All ICT support requests will be issued with a ticket number. Support requests can be raised by logging a call on Top desk or emailing support@sut.gdst.net

For urgent requests, they can be contacted on: Ext 33011 or by radio. (Contact Reception for assistance in radioing ICT). Ext 33011 is redirected to IT Staff work mobile phones during working hours.

6. Teams and the GDST hub

All girls have lesson materials stored via Microsoft Teams, to allow them to access this for revision or if a lesson is missed for any reason. All homework in Senior School is set via Assignments in Microsoft Teams.

A GDST Intranet is available to provide GDST wide information and collaboration between schools. This can be access via the following link

https://gdst.oak.com/

The Hub contains the legal information, GDST policy and guidance in a range of areas.

7. Resources and Room Booking

It is possible for staff to book ICT rooms and resources such as laptops, iPads and cameras from around the school.

The booking system can be accessed via the following link

https://suttonhigh.roombookingsystem.co.uk

8. Encryption

All USB sticks that have GDST data on them will be required to be encrypted. Non encrypted USB sticks will only be able to be read in GDST computers and not written to.

Encrypted USB sticks can be read in any Windows computer and are protected by a password. If the password is forgotten, it can be reset using any computer within school.

9. Phishing and scam email training

Users will not be penalised for genuine mistakes when using GDST digital technology. Phishing attacks are a common tactic used by cybercriminals to steal sensitive information such as logins or passwords or install ransomware and 90% of cyberattacks are made possible by human error. We already use a number of technical security controls to reduce this threat, for example we use an email gateway, deploy anti-virus software, and we have sophisticated tools to detect anomalies within our system but on their own these tools can never be 100% effective.

To counter this ongoing threat, we are running an awareness campaign, which includes an informational video followed by a number of phishing simulation emails, which we will send to staff over the course of the year to provide you with a hands-on opportunity to recognise and respond to phishing attempts. Please be assured that this is not an exercise designed to catch anyone out. Don't worry if you click on the phishing simulation links though, you will simply be taken to some further training to help you spot them in the future.

As always, be cautious when receiving emails from unexpected sources, with unusual links, attachments, urgency or requests as you may still receive real phishing emails during our awareness campaign. If you receive a phishing email, report it using the 'message actions' button on the email ribbon which is shown below (not IOS) otherwise delete it. If you are concerned you have clicked on a link, opened an attachment or provided sensitive information (and you weren't directed to our training) notify your IT team as normal.

If I suspect I may have clicked a link in a phishing email in error, downloaded a suspicious file, or inadvertently allowed a third-party access to any GDST system, account, application or network I will immediately notify a member of the IT team.

Appendix A

Protecting data - what you need to consider

Away from school

Taking data home from school

You may need to take data out of school when you work from home or go on a trip. Don't be careless with data; laptops and USB sticks should be encrypted and hard copy folders or mark books should be kept securely. You **must not** store data on personal computers or laptops that are not encrypted.

Using your mobile device

Always use your school email address to send emails from home. Any mobile device that is being used to access school emails or SIMS **must be password protected**.
Consider waiting until you have access to a desktop or laptop to send information as checking email addresses and contents are correct before you send it on is hard to do on a mobile phone.

Opening emails

Checking email from your phone can sometimes be dangerous as you may not be able to see the full sender information. If you don't know the source, don't open it. If you suspect something may be malicious, report it to ictsupport@sut.gdst.net.

Talking

Watch what you are saying and how loudly you're speaking. There could be people listening nearby who could overhear any sensitive discussions that may be classed as 'personal data'.

At school

Leaving information unattended

Be careful not to leave your laptop open or PC screen visible. Remember to lock your system screens when leaving them unattended in the classroom, and shut down fully at the end of the day before heading home.

Sending secure emails from school

Only use the school email system to ensure emails are sent securely.
Do not include attachments that may contain any personal data, instead include a hyperlink to a file location where this information can be accessed. Restrictions on these folders will prevent access to personal data to anyone without the correct permissions.

Personal or sensitive data

If you hold personal or sensitive data (pupil names, SEN information etc) whether on paper or electronically make sure it is kept securely.
Do not share data unless there is a justified reason, and if it does need sharing use a hyperlink to a secure file location.

Transferring personal data

If you need to send personal data to a third party (eg pupil details for trips) wait until you are positive the school has a contract in place. Use a secure transfer solution such as OneDrive, or password protect files and send the password under separate cover.

Archiving outdated files

Archive or delete any data that is no longer needed. There is no business reason to hold data on pupils after the age of 25.

Disposing of confidential data

Do not leave sensitive or confidential papers lying around, be sure to lock them away or, if you do not need them anymore, shred them.

Appendix B

STAFF ICT ACCEPTABLE USE AGREEMENT

I understand that working in an educational context brings with it high expectations of behaviour and integrity, and responsibilities with regard to safeguarding. This agreement covers these expectations in the context of the use of all digital technologies and equipment provided by the GDST regardless of the time at or location in which they are being used.

I acknowledge that these rules will help to keep everyone safe and that GDST systems and users are protected and monitored by security and filtering services, to provide safe access to digital technologies and the internet. These expectations include:

- Interacting with pupils in an appropriate way.
- Interacting with colleagues, parents, and other school or work contacts in an appropriate way.
- Being trustworthy with confidential and sensitive information.
- Looking after the fabric and equipment of the school and the GDST, and respecting school property.
- Maintaining the reputation of the school and the GDST (even when not at work).
- Maintaining professional standards of conduct.

These things are equally true when ICT systems, including computers and phones, are involved.

Staff may use school/GDST equipment/network for:

- School/work purposes.
- Reasonable personal use that does not interfere with work.

I understand:

- it is my duty to support a whole-school safeguarding approach and I will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff or Designated Safeguarding Lead.
- GDPR / Data Protection training is mandatory for all GDST employees. I will comply with data protection law, and the GDST data protection and information security policies and procedures which are accessible to me on the GDST knowledge hub.
- I will not be penalised for genuine mistakes when using GDST digital technology. If I suspect I may have clicked a link in a phishing email in error, downloaded a suspicious file, or inadvertently allowed a third-party access to any GDST system, account, application or network I will immediately notify a member of the IT team.
- that my behaviour online using GDST devices whether in school, Trust Office or elsewhere, may be subject to monitoring and may be accessed to meet business needs.

I will not:

- allow other people to access or use any personal user account provided to me by the GDST or log onto any device using my GDST credentials.
- use the GDST password or personal credentials of another member of staff.
- engage in any online activity that might compromise my professional status or responsibilities or bring the GDST into disrepute.
- use GDST's technology or equipment to support or promote extremist organisations, messages or individuals and I will not browse, download or send material that is considered offensive or of an extremist nature by the GDST. I will follow the standards set out in the GDST Safeguarding Procedures.
- intentionally download or run any software or resources from the internet that can compromise the GDST IT network or might allow me to bypass the filtering and security system. I will not connect any device to the GDST network that does not have up-to-date anti-virus software.
- I will not: use my personal email for school or GDST business and will not transfer GDST files or documents containing the personal information of pupils, parents or staff, or GDST sensitive business information onto them.
- I will not: use personal messaging apps (for example WhatsApp) to share personal information of staff, students, alumnae or parents, or to communicate with students
- store GDST sensitive information on my own devices, data storage device or cloud storage area. I will not use personal digital recording devices for taking, editing or transferring images or videos of pupils(*).

(*) If I have a relative who is a GDST pupil, this obligation applies only where I am acting in a school capacity.

I will:

- Bring to the attention of the ICT Department or a member of the Senior Leadership Team any ICT activity or material that may be inappropriate or harmful.
- Report any damage or faults involving equipment or software, however this may have happened, as soon as reasonably possible.
- Only use chat and social networking sites in accordance with the school's and GDST's policies.
- Only communicate with pupils using GDST email, work phones, and other school communication systems, but not personal phones, email, or social media, except in an emergency, in order to protect both pupils and staff.
- As far as is possible, use GDST provided systems to communicate with parents on school and pupil matters. I will maintain professional standards of conduct if I communicate with parents socially using personal phones, email or social media.

Information Security

I understand that I may have access to sensitive information about colleagues, families or pupils in our care. I will comply with the GDST guidance on data protection and will keep sensitive information within the GDST network. I will not send sensitive information via personal email accounts (Hotmail, GMail etc) or store it on:

- Un-encrypted USB sticks
- Personal devices (phones, laptops) or
- 'Cloud storage' (iCloud, personal Onedrive, Dropbox, personal GoogleDrive)

Note that cloud storage (OneDrive / Sharepoint) provided by GDST is permitted to be used for storage.

I will comply with security requirements that may be required to maintain the security of GDST systems. This includes using Multi Factor Authentication (MFA) to protect my staff account, and if requested in the future on student accounts.

Images & Videos

In order to prevent allegations of inappropriate activities, I will not store images of pupils on my personal devices. Any images taken on personal devices (including in EYFS) will be downloaded to school or GDST systems as soon as reasonably possible and the personal copy permanently removed.

Bringing Your Own Device

When I use personal devices in work, I understand that the same expectations of behaviour apply as if I were using school equipment.

I understand that if I fail to comply with this Acceptable Use Agreement, I may have my ICT access suspended and/or be subject to disciplinary action. A copy of this agreement is available upon request and is available within Oracle. I understand a copy of this signed document will be placed on my personal file.

I have read and understand the above.

APPENDIX C

Secondary Pupil Acceptable Use Agreement / eSafety Rules

Online behaviour

- ✓ I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes. I will keep to the school rules when using my own devices.
- ✓ I will not download or install software on school ICT equipment without permission.
- ✓ I will only log on to the school network/ learning platform with my own user name and password.
- ✓ I will follow the schools ICT security system and not reveal my passwords to anyone.
- ✓ I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible. I will never post aggressive or offensive material on the system or the web at any time.
- ✓ I will respect the privacy and ownership of others' work on-line at all times.
- ✓ I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff.
- ✓ I will not attempt to bypass the internet filtering system.
- ✓ I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.
- ✓ I acknowledge that external email communication beyond the GDST domain is prohibited, except for correspondence from pre-approved senders (e.g., Microsoft Teams) and for students in Years 10-13 who have external email privileges.
- ✓ **I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent / guardian may be contacted.**

Online safety at all times.

- ✓ I will be very careful about giving out personal information such as name, phone number or address online. I will not post my information in a social network profile so that anyone can see it.
- ✓ I will not arrange to meet someone I only know online unless my parent / guardian / teacher has clearly approved of this.
- ✓ I understand that online contacts may lie about their identity. I know that information on the web can be unreliable. I will be very cautious about who and what I believe.
- ✓ Images of pupils and / or staff will only be taken, stored and used for school purposes in line with school policy. I will not distribute images outside the school network without permission.
- ✓ I will support the school approach to online safety and not deliberately upload or send any text, images, video, or sounds that could upset or offend any member of the school community
- ✓ I understand that all my use of GDST systems is monitored and logged and can be made available to my teachers.
- ✓ **If anything makes me uncomfortable or worried, I know that I can share this with a member of staff or parent without being blamed.**

Bringing your own device.

- ✓ I will use the device **solely for educational purposes**;
- ✓ I will not plug my personally owned device into the wired network.
- ✓ I will get my device's charger PAT Tested by the ICT Team before using it in school.
- ✓ I will only use the "GDST Guest" or GDST-BYOD wifi access when connecting to the network.
- ✓ I will seek approval from a member of staff **before** getting a device out in class.
- ✓ I am aware that I will be subject to the school's internet filtering policies.
- ✓ I will take sole responsibility for my device. I understand that in the event the device is lost, stolen or damaged while on the school premises, the school does not accept any responsibility.
- ✓ Devices will not be covered by the GDST insurance policy.
- ✓ The school will provide instructions to access the "GDST Guest" or GDST-BYOD wifi on a best-efforts basis, however, if my device malfunctions, it is **not** the responsibility of any member of staff to fix it.