Damers First School

Staff ICT and Electronic Devices Policy

Date policy last reviewed: September 2023

Signed by:

________________________ Head of School Date: ________________________

________________________ Chair of governors Date: ________________________

Contents:

Appendices

Statement of intent

Damers First School believes that ICT plays an important part in both teaching and learning over a range of subjects. The school is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

The school has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the internet.
- School ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.

Personal use of ICT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, the Social Media Policy and Online Safety Policy.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Cyber Response Plan

2. Roles and responsibilities

The governing board has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The Head of School is responsible for:

- Reviewing and amending this policy with the ICT Technician and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources. This duty is carried out daily by the ICT Technician.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Informing staff that the school reserves the right to access school-owned devices for the purpose of ensuring the effectiveness of this policy.

The ICT Technician is responsible for:

- Carrying out checks on internet activity of all user accounts and to report any inappropriate use to the Head of School, DSL or IT lead.
- Monitoring the computer logs on the school's network and to report any logged inappropriate use to the Head of School.
- Remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.

- Ensuring routine security checks are carried out on all school-owned devices that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks.
- Accessing files and data to solve problems for a user, with their authorisation.
- Adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers.
- Disabling user accounts of staff who do not follow this policy, at the request of the Head of School.
- Assisting the Head of School in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the ICT facilities and devices, if required.
- Immediately reporting any breach of school owned devices to the DPO and the Head of School.

The DPO is responsible for:

- Ensuring that all school-owned devices have security software installed, to protect sensitive data in cases of loss or theft.
- Ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy.
- Ensuring that all devices connected to the school network and internet are encrypted.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.

Staff members are responsible for:

- Ensuring that all personal devices that are used to access school IT systems have security software installed, to protect sensitive data in cases of loss or theft.
- Requesting permission from the Head of School or ICT Technician, subject to their approval, before using school-owned devices for personal reasons during school hours.
- Requesting permission to loan school equipment and devices from the Head of School or ICT Technician.
- Reporting misuse of ICT facilities or devices, by staff or pupils, to the Head of School, ICT Lead or ICT Technician.
- Reading and signing a Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

The ICT Technician is responsible for the maintenance and day-to-day management of the equipment, as well as the device loans process.

The ICT Lead, ICT Technician, Head of School and School Finance Officer are responsible for:

- Maintaining a Fixed Asset Register to record and monitor the school's assets.
- Ensuring value for money is secured when purchasing electronic devices.

- Monitoring purchases made under the Finance Policy.
- Overseeing purchase requests for electronic devices.

3. Classifications

School-owned and personal devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software
- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Equipment located in the sensory room
- Documents and publications (any type of format)

4. Acceptable use

This policy applies to any computer or other device connected to the school's network and computers.

The school will monitor the use of all ICT facilities and electronic devices. Members of staff will only use school-owned and personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Taking photographs (school-owned devices only)
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school office for assistance.

Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy.

Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

Any member of staff found to have breached the school's Data Protection Policy or relevant legislation will face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

Since ICT facilities are also used by pupils, the school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

Pupils found to have been misusing the ICT facilities will be reported to the Head of School.

School-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Any illegal, inappropriate or harmful activity will be immediately reported to the Head of School.

Members of staff will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files (over 500MB) without permission from the ICT Technician.
- Give their home address, phone number, social networking details or personal email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.
- Take mobile phones used for communication on school trips out of the school premises, unless permitted by the Head of School.

All data will be stored appropriately in accordance with the school's Data Protection Policy.

Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent.

School-owned electronic devices will not be used to access personal social media accounts.

Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the school online.
- Avoid disclosing any confidential information or comments regarding the school, or any information that may affect its reputability.
- Avoid disclosing any information regarding their role on social media that may increase their risk to cyber phishing.
- Have the necessary privacy settings applied to any social networking sites.

Images or videos of pupils or staff will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.

School-owned devices will be taken home for work purposes only, once approval has been given by the Head of School and ICT Technician. Remote access to the school network will be given to staff using these devices at home.

School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the Head of School.

While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the Head of School or in the case of a personal emergency.

Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Use of a school-owned phone for short personal use will be permitted for necessary calls. Should staff need to use the telephones for a longer call, authorisation will be sought from the Head of School. This authorisation will be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls; however, staff will notify the Head of School after the call.

Personal use of school-owned equipment can be denied by the Head of School at any time. This will typically be because of improper use or over-use of school facilities for personal reasons.

Where permission has been given to use the school equipment for personal reasons, this use will take place during the employee’s own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member’s work, and the work of others, is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, will be reported to the Head of School.

More details about acceptable use can be found in the staff Technology Acceptable Use Agreement.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. Emails and the internet

The school email system and internet connection are available for communication and use on matters directly concerned with school business.

Emails will not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be proofread by the staff member sending the email to ensure this prior to sending.

Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.

The school will be liable for any defamatory information circulated either within the school or to external contacts.

School email accounts will never be used to subscribe to spam or other non-work-related updates, advertisements or other personal communications. School email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

All emails that are sent or received will be retained within the school for a period of ten years dependent on the information contained, according to the school's Retention Schedule.

All emails being sent to external recipients will contain the school standard confidentiality notice. That notice will normally be configured as a signature by the ICT Technician and will not be removed.

Personal email accounts will only be accessed via school computers outside of work hours. Staff will ensure that access to personal emails never interferes with work duties.

The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.

Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.

Purchases for school equipment will only be permitted to be made online with the permission of the Head of School, and a receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase will be made for the purchaser and the Finance Officer. This is in addition to any purchasing arrangement followed according to the school's Finance Policy.

6. Portable equipment

All data on school-owned equipment will be stored in the cloud.

Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and stored away from children when they are not in use.

Portable equipment will be transported in its protective case, if supplied.

Where the school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, staff will only use these devices.

7. Personal devices

Staff members will be able to use personal devices in school in line with the school's Cyber Response Plan.

Approved devices will be secured with a password or biometric access control, e.g. fingerprint scanner.

Members of staff will not contact pupils or parents using their personal devices.

Personal devices will only be used for off-site educational purposes when mutually agreed with the Head of School.

Inappropriate messages will not be sent to any member of the school community.

Personal devices will not be used to take any photographs or videos of pupils.

Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.

During lesson times, unless required for the teaching activity being undertaken, personal devices will be kept in a space where it cannot be seen or accessed by pupils.

8. Removable media

At Damers First School we do not use removable media for storage of school data. If the use of removable media is necessary for reasons other than that of storage of school data (ie storage of resources) the equipment must be checked by the ICT Technician prior to use.

9. Cloud-based storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

10. Storing messages

Any emails downloaded and stored on school-owned or personal devices or in a hard copy file must be disposed of after no more than ten years in accordance with the school's Retention Schedule.

Information and data on the school's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

If a member of staff is unsure about the correct message storage procedure, help will be sought from the ICT Technician.

Employees who feel that they have cause for complaint as a result of any communications on school-owned devices will raise the matter initially with the Head of School, as appropriate. The complaint will then be raised through the grievance procedure in line with the Grievance Policy.

11. Unauthorised use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the Head of School.
- Physically damage ICT and communication facilities or school-owned devices.
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the ICT Technician or Head of School. Certain items are asset registered and security marked; their location is recorded by the ICT Technician for accountability. Once items are moved after authorisation, staff will be responsible for notifying the ICT Technician of the new location.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password will be changed every three months. User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
    - Online gambling
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the ICT Technician or the Head of School.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, override or overwrite the security parameters on the network or any of the school's computers.
- Use or attempt to use the school's ICT facilities to undertake any form of piracy, including the infringement of software licences or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any ICT facilities without the consent of the ICT Technician or Head of School. This is in addition to any purchasing arrangements followed according to the Finance Policy.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the Head of School. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff will not download or attempt to download any software of this nature.

- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the ICT facilities for personal use during work hours without the authorisation of the Head of School. This authorisation will be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member it is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of the Head of School.
- Obtain and post on the internet, or send via email, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Disciplinary Procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they will report this immediately to the Head of School.

12. Staff issued electronic devices

School equipment, including electronic devices, will be issued to some staff members.

Equipment and devices will only be issued to staff members who have read, signed and returned the terms of use, as set out in the Staff Declaration Form (appendix 1).

By loaning school equipment and electronic devices, staff members will be agreeing to act in accordance with the terms of acceptable use.

Staff members will be required to store, handle and update any device loaned to them appropriately.

If the equipment or device is no longer required, or upon leaving employment of the school, staff members will return the equipment to the ICT Technician as soon as possible, allowing the equipment to be made available to someone else.

Devices allowed for loan will be encrypted and protected to ensure the security of any data they hold.

13. Purchasing

Requests for equipment or electronic devices will be made in writing to the Finance Officer, ICT Lead or ICT Technician.

Requests will be submitted in sufficient detail for an informed decision to be made.

Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on the school's behalf unless permission has been sought from the Head of School.

The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the school, unless otherwise specified by the Head of School.

In relation to devices for a specific project, project budget holders will provide evidence and a written statement requesting the necessary funds for the equipment required.

The Finance Officer will seek advice from the ICT Lead or ICT Technician and professionals when purchasing equipment.

All equipment and electronic devices will be sourced from a reputable supplier.

The ICT Technician will maintain a Fixed Asset Register which will be used to record and monitor the school's assets. All equipment and electronic devices purchased using school funds will be added to this register.

When devices are not fit for purpose, staff members may request new equipment. If their request is granted, the old equipment or electronic device will be returned to the ICT Technician, including any accessories which were originally included with the device. Any old devices will then be disposed of or wiped clear by the ICT Technician.

14. Safety and security

The school's network will be secured using firewalls in line with the Cyber Response Plan.

Filtering of websites, as detailed in the Cyber Response Plan and the Online Safety Policy, will ensure that access to websites with known malware are blocked immediately and reported to the ICT Technician.

Approved anti-virus software and malware protection will be used on all approved devices and will be updated automatically by the software provider.

Members of staff will ensure that all school-owned electronic devices are updated when an update is available. Computers will be shutdown fully at the end of each working day to ensure any updates or patches requiring a reboot for installation to be installed.

Staff using personal devices to access school systems or email accounts will update them as required so that appropriate security and software updates can be installed to prevent any loss of data.

Programmes and software will not be installed on school-owned electronic devices without permission from the ICT Technician.

Staff will not be permitted to remove any software from a school-owned electronic device without permission from the ICT Technician.

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the ICT Technician, may be subject to disciplinary measures.

All devices will be secured by a password or biometric access control.

Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Devices will be configured so that they are automatically locked after being left idle for a set time. This will be no more than 15 minutes for desktop computers or laptops.

All devices must be encrypted using a method approved by the DPO.

Further security arrangements are outlined in the Online Safety Policy and Cyber Response Plan.

15. Loss, theft and damage

For the purpose of this policy, **"damage"** is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT Technician
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

The school's insurance will cover school-owned electronic devices that are damaged or lost, during school hours, if they are being used on the school premises.

Staff members will use school-owned electronic devices within the parameters of the school's insurance cover – if a school-owned electronic device is damaged or lost outside of school hours and/or off-site, the member of staff at fault may be responsible for paying damages.

Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.

The ICT Technician and Head of School will decide whether a device has been damaged due to the actions described above.

The ICT Technician will be contacted if a school-owned electronic device has a technical fault.

The member of staff will not be permitted to access school-owned electronic devices until the payment has been made.

In cases where a member of staff repeatedly damages school-owned electronic devices, the Head of School may decide to permanently exclude the member of staff from accessing devices.

If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the school, its staff and its pupils, and that the loss is reported to the relevant agencies.

The school will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

16. Implementation

Staff will report any breach of this policy to the Head of School.

Use of the school internet connection will be recorded and monitored.

The ICT Technician will conduct yearly checks of asset registered and security marked items.

Unsuccessful and successful log-ons will be logged on every computer connected to the school’s network.

Unsuccessful and successful software installations, security changes and items sent to the printer will also be logged.

The ICT Technician may remotely view or interact with any of the computers on the school’s network. This may be used randomly to implement this policy and to assist in any difficulties.

The school’s network has anti-virus software installed with a centralised administration package; any virus found will be logged to this package.

The school’s information management system (SIMS) is computerised. Unless given permission by the Head of School, members of staff will not access SIMS. Failure to adhere to this requirement may result in disciplinary action.

All users of SIMS will be issued with a unique password. Staff will not, under any circumstances, disclose this password to any other person.

Attempting to access the database using another employee’s user account and/or password without prior authorisation will likely result in disciplinary action, including summary dismissal.

User accounts will be accessible by the ICT Technician.

Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

17. Monitoring and review

This policy will be reviewed every two years by the ICT Lead, ICT Technician and the Head of School.

Any significant changes or amendments to this policy will be communicated to all staff members by the ICT Lead, ICT Technician or the Head of School.

The scheduled review date for this policy will be Nov 2024.

Appendix 1

Staff Declaration Form

All members of staff are required to sign this form before they are permitted to use electronic devices that are owned by the school.

By signing this form, you are declaring that you have read, understood and agree to the terms of the Staff ICT and Electronic Devices Policy. You should read and sign the declaration below before returning it to the ICT Technician.

Members of staff are required to re-sign this declaration form if significant changes are made to the policy.

I have read the school's Staff ICT and Electronic Devices Policy and understand that:

- School equipment must not be used for the fulfilment of another job or for personal use, unless specifically authorised by the Head of School.
- Illegal, inappropriate or unacceptable use of school or personal equipment will result in disciplinary action.
- The school reserves the right to monitor my work emails, phone calls, internet activity and document production.
- Passwords must not be shared and access to the school's computer systems must be kept confidential.
- I must act in accordance with this policy at all times.

Name of staff	
Job title	
Signed	
Date signed	