DULWICH COLLEGE
FOUNDED 1619

ICT ACCEPTABLE USE POLICY (STAFF)

1. **Overview**

Dulwich College has an established culture of openness, trust and integrity. The College is committed to protecting its pupils, staff and itself from illegal or damaging actions by individuals, carried out either knowingly or unknowingly.

All staff should familiarise themselves with this document in order to protect themselves, pupils, colleagues and the College against potential harm which may arise from the misuse of any of its information and communications technology (ICT) systems including its network, email and internet facilities.

Advances in the use of ICT in the classroom and in the workplace, and in response to periods of lockdown, have led to changes in the way many staff members work, in particular use of the internet, email and mobile technology. Staff are expected to have a positive and flexible approach to using ICT to support teaching and learning and in the administration of the College's activities. The College supports the use of ICT by staff in a manner that is innovative without harming any of its systems or obstructing the work of others.

2. **Purpose**

The purpose of this policy is to outline what constitutes acceptable use of the College's ICT systems and its computer equipment/devices by the staff of Dulwich College. The advice and restrictions are intended to protect both the staff member and the College. Inappropriate use exposes Dulwich College to risks including virus attacks, possible threats to networked systems and services, and legal issues. Some staff, in particular those administering the network, may at times be exempted from some of these restrictions during the course of their legitimate job responsibilities.

This policy outlines the standards the College expects of the users of the systems/equipment and the action it will take in respect to breaches.

3. **Scope**

This policy applies to all individuals working at Dulwich College (including contractors, consultants, temporary staff, casual workers, agency staff and volunteers). Third parties (e.g. hirers and visitors) who have access to any of the College's ICT systems or equipment are also required to comply with this policy.

This policy applies to all equipment/devices that are owned, leased, hired or otherwise used by Dulwich College, whether on or off College premises.

This policy applies to ICT systems which includes all computer systems (internet, email, etc.) software or hardware including any computer or associated peripheral, wireless or mobile device provided by the College

as well as devices which may be owned by individuals whilst they are connected to the Dulwich College network.

4. Responsibility for implementation of this Policy

The College Leadership Team has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the Head of Computer Services. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to the operations of the College lies with the Head of Computer Services and the College Leadership Team.

Computer Services will deal with requests for permission or assistance under any provisions of this policy, subject to their primary tasks of maintaining the core systems of the College and may specify certain standards of equipment or procedures to ensure security and compatibility.

All managers have a specific responsibility: (a) to operate within the boundaries of this policy; (b) to ensure that the employees who report to them understand the standards of behaviour expected of them; and (c) to report and take action when breaches occur.

Any misuse of the College's ICT systems or equipment must be reported to the Head of Computer Services.

Questions regarding the content or application of this policy should be directed to the Head of Computer Services, the Chief Operating Officer or the Deputy Master Pastoral & Co-Curricular.

5. Policy

5.1 General Use

All users should be aware that the data they create on the College ICT systems remains the property of Dulwich College. While the Computer Services Department strives to maintain a high degree of information security for data stored on, or transmitted over the College infrastructure, no absolute guarantee of confidentiality or integrity can be given for such data. Consequently, users must exercise due care and judgment regarding the sensitivity of the information they store or transmit using these facilities.

All users must register to use the College ICT systems including the network by obtaining a logon name and password. The provision of these constitutes a right to access College ICT systems under the terms of this policy. Staff must ensure that the Computer Services Department is informed of any change to their role which may affect their level of access permission and right to use specific systems.

On ceasing to be employed by the College a staff member's account is automatically disabled; any staff member wishing to have continued access on a temporary basis, for example to email and documents, should submit a request to the Head of Computer Services.

All computer equipment loaned or provided by the College should be returned to the Computer Services Department before a staff member leaves.

Staff are responsible for exercising good judgment regarding the reasonableness of personal use of the College's applicable ICT systems such as the internet and phone.

5.2 **Devices provided by the College**

Any member of staff who is provided with a College device for the purposes of their role are expected to use it in accordance with this policy (and any agreement that they sign on taking receipt of the device from the Computer Services Department).

Staff must inform the Computer Services Department immediately in the event any device provided by the College is lost, damaged or compromised in any way.

5.3 **Security, Passwords and Proprietary Information etc.**

5.3.1 **Security**

Staff who have been issued with a College device must ensure that it is kept secure at all times, especially when travelling and must not allow it to be used by anyone other than in accordance with this policy. Passwords must be used to secure access to data kept on such devices to ensure that confidential and personal data is protected in the event of loss or theft.

If staff are accessing College systems via their personal devices, those devices should be password protected and if they are shared use devices, staff must ensure they have logged out of any College systems when they are no longer working on the device.

Staff should also be aware that when using any devices away from the workplace, email or documents may be read by third parties, for example, passengers on public transport.

No College information (confidential or personal) or electronic documents should be copied to or stored on any other portable storage devices (such as flash drives, portable hard drives, CDs or DVDs). Data should be stored on the College network, a staff member's College OneDrive account or within a shared Team.

If staff are authorised to have access to any College systems, they are responsible for the security of information accessed via devices. On leaving a device unattended they should ensure that they lock their device or log off to prevent unauthorised users accessing systems or viewing confidential/personal data in their absence. Staff without authorisation should only be allowed to use computers under supervision.

Desktop PCs, cabling for telephones, switches, routers or computer equipment should not be moved or tampered with without first consulting Computer Services.

5.3.2 **Passwords**

Passwords should be unique to a member of staff's College account and must not be used for other systems. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Head of Computer Services. For the avoidance of doubt, on the termination of employment (for any reason)

staff must provide details of their pincodes and passwords to the Head of Computer Services and return any College owned devices, key fobs or cards (as applicable).

5.3.3 **Appropriate Access to Systems/Network**

Users are given access to those systems and areas of the College network appropriate to their job; staff should not attempt to gain unauthorised access to systems or parts of the network which are blocked.

Users must take care not to damage, amend or corrupt data or data structures. Users must take care not to knowingly introduce viruses or other harmful programs or files. When connecting external storage devices, or other electronic equipment staff must take care not to introduce viruses.

Staff must obtain prior authorisation from the Computer Services Department prior to:

- purchasing (or otherwise installing or introducing) any new software/app etc., for use on any part of the College's ICT systems; or
- plugging any device (for example a home computer) directly into the College's network (e.g., via a docking station)

to permit the Computer Services Department to check the impact of that device/app etc. on the integrity of the College's systems. (NB: It is permissible to use a personal device with the College's Wi-Fi).

Staff may not download software for which no license is held.

If any harm is done to any ICT system accidentally, users should inform Computer Services immediately.

5.3.4 **Suspected Breach of the system**

If a staff member suspects there has been a breach in the College network or any damage has been done to any part of the ICT systems or that there has been any illegal tampering or surveillance of the College network, this must be reported immediately to Computer Services.

5.3.5 **Confidentiality and Data Protection**

Confidential Information: Much of the information stored on the College's ICT systems is of a confidential nature and should not be disclosed to outside parties. Printouts of documents containing confidential information should be securely disposed of.

Personal Information: Staff will handle a lot of personal information (information relating to pupils/parents/colleagues etc.) and they are obliged to ensure that data is processed, shared and retained in accordance with the Data Protection Act 2018 and the College's Data Protection Policy. In particular, staff are reminded that they should inform the Clerk to the Governors at legal@dulwich.org.uk immediately if they become aware of: (1) a personal data breach; and/or (2) a potential subject access request.

In the interests of confidentiality and protection of personal information, all College business must be conducted on the College systems; staff are not permitted to use personal email accounts for work purposes and personal devices/personal cloud-based storage areas should not be used to store any information/documents relating to College business. Furthermore, staff should not enter any staff/pupil etc. personal data onto any Artificial Intelligence tools.

5.3.6 **Private personal information**

Staff should be cautious about protecting their own private personal information while using the College ICT systems. Documents containing information of a personal nature, such as financial or medical matters, should not be stored on the College network. Staff are cautioned not to divulge any of their personal information to anyone on the internet or via email or any other form of electronic communication. Access to online financial institutions or internet shopping is strongly discouraged while connected to the College network.

Staff should take care when uploading material to such sites which might bring either the individual or the College into disrepute.

5.3.7 **Digital images**

Staff should exercise caution when using, copying or transferring digital images or photographs of the College, pupils, grounds or other staff members.

With a few exceptions, all parents agree on their child joining the College that their photos may be used for marketing and publicity purposes. The Communications Department hold a list of those pupils for whom permission has been withheld and this should be checked before publishing any photograph online. Staff should also refer to the College Policy on the Taking and Use of Photographs of Pupils.

Explicit permission must be obtained prior to publishing or causing to be published images of the College, staff or pupils in the press, on third-party websites, social networking sites (save for College social media channels), or before emailing them to any third party.

If a member of staff has any doubts about the circumstances under which a photograph or image (of the College, member of staff or pupil) may be used they should contact the Communications Department.

Photographs taken of College events or trips/expeditions should be transferred and stored in the College's central archive of digital images.

5.3.8 **Email**

The College monitors all e-mails passing through its systems for viruses. Staff should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious. Computer Services should be informed immediately if a suspected virus is received. The College reserves the right to block access to attachments to e-mails for the purpose of effective use of the system and for compliance with this policy. The College also reserves the right not to transmit any e-mail message.

The use of email is considered by the College to be a standard means of communication. All staff are expected to check their email at least once a day.

Email messages sent outside the College network contain a standard disclosure statement outlining the College's security and confidentiality policy. A copy of this can be requested from the Computer Services Department.

Staff should not:

- send abusive, obscene, discriminatory, racist or otherwise offensive emails;
- send or forward private e-mails at work which they would not want a third party to read;
- e-mail text, music and other content on the internet that is subject to copyright protection, unless it is clear that the copyright owner allows this;
- send messages from another employee's email account or under an assumed name unless specifically authorised to do so.

Staff should:

- assume that any e-mail message may be read by others;
- where possible use the relevant distribution groups to communicate with colleagues; mass emails to all staff should be avoided;
- adhere to the same College standards when using email as with other forms of written communication, particularly if the message is addressed to recipients outside the College;
- always communicate with current pupils using their college email account. They should also only email pupils using the pupil's College email account.

Staff who receive a wrongly delivered e-mail should return it to the sender.

Staff should be mindful that email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

5.3.9 **Third-Party Email Services**

Dulwich College has all messages to or from its own email accounts screened for viruses or other destructive code. However, this protection is not available for other mail services such as Hotmail, and care should be exercised when using these from the College network. In particular, extreme caution must be exercised when opening email attachments whilst using those other email services. If in any doubt about the nature of a message from an unknown source, the email should not be opened and should be deleted immediately.

5.3.10 **Social Networking Sites**

Detailed guidance on setting up and running a College social media site and using personal social media is set out in the College's Social Media Policy and the document "Creating a Social Media Site". In particular, staff should not accept invitations from current pupils to become 'friends' on social networking sites.

5.3.11 **Copyright**

Under no circumstances may staff or pupils of Dulwich College engage in any activity that is illegal under UK or international law whilst logged onto the College network or using College-owned equipment. This includes violations of copyright or intellectual property rights, such as the illegal downloading of music, videos or unlicensed software. Information about copyright-cleared resources is available from the Libraries or from the Computer Services Department.

5.3.12 **Commercial activity**

Users must not use any College ICT systems for commercial gain or self-promotion without the specific authorisation of the appropriate manager. Users are prohibited from making fraudulent offers of products, items, or services originating from any Dulwich College account.

5.3.13 **Staff Training**

Staff are required to undertake mandatory cyber security training (and complete the associated courses) within the timescales set by the Computer Services Department from time to time.

6. **Personal use of ICT systems**

The College permits the incidental use of internet, e-mail and telephone systems to send personal e-mails, browse the internet, access social media, and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. The College reserves the right to withdraw its permission at any time.

The following conditions must be met for personal usage to continue: (a) use must be minimal and take place substantially out of normal working hours; (b) use must not interfere with work commitments; and (c) personal international telephone calls must not be made.

Staff should be aware that personal use of the College's ICT systems may be monitored (see below) and, where breaches of this policy are found, disciplinary action may be taken. The College reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers personal use to be excessive.

7. **Monitoring use of ICT systems**

The College's systems enable it to monitor/access telephone, e-mail, voicemail, internet and other communications. Monitoring is only carried out to the extent permitted or as required by law and as necessary

and justifiable for College purposes including for security, safeguarding, and/or network maintenance purposes.

In particular, the College reserves the right to retrieve the contents of emails and to check internet usage for the following purposes (this list is not exhaustive):

- to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of wrongful acts; or
- to comply with any legal obligation.

Certain websites are automatically blocked by the College's filtering system, which is reviewed on a regular basis by the Deputy Head Pastoral and Co-Curricular and Assistant Head Safeguarding. If a website being blocked causes problems for work / research purposes, staff should contact the Head of Computer Services for assistance. Staff should report to the Deputy Master Pastoral & Co-Curricular if they accidentally access materials of a violent or sexual nature whilst using College ICT systems. The proxy server records attempts to access undesirable sites from any device connected to the College network whether hard-wired or wireless and daily reports of these attempts are regularly reviewed by the Deputy Head Pastoral and Co-Curricular and Assistant Head Safeguarding (who will then liaise with the Head of Computer Services should additional websites need to be blocked).

Devices which belong to the College and are used by members staff have SECURUS installed on them. This monitors the use of the device whether on or off College premises.

A CCTV system monitors various areas of the campus. This data is recorded.

8. **Inappropriate use of ICT systems and equipment**

Misuse or excessive use or abuse of the telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with under the College's Disciplinary Procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence.

Staff must not use the College's ICT systems or equipment to participate in online gambling or to create, view, access, transmit or download any of the following:

- pornographic or obscene material;
- material which is discriminatory, offensive, derogatory or may cause offence or embarrassment to others;
- any defamatory statement about any person or organisation or material which is discriminatory;

- confidential information which they do not have authority to access; and
- material in breach of copyright.

Any such action will be treated very seriously and may result in summary dismissal for gross misconduct.

Where evidence of misuse is found the College may undertake a more detailed investigation, involving the examination and disclosure of information to those undertaking the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary information may be handed to the police in connection with a criminal investigation.

9. Enforcement

Any member of staff found to have violated this policy may be subject to disciplinary action.

10. Related Policies

Staff should never access or use the College's ICT systems or College ICT equipment/devices in a way that breaches any of the College's policies. This policy should be read in conjunction with the following policies:

- Staff Code of Conduct
- Social Media Policy
- Data Protection Policy
- Data Security Policy
- Privacy Notice for Staff
- Privacy Notice for Pupils, Parents and Old Alleynians
- College Policy on the Taking and Use of Photographs of Pupils
- Safeguarding (Child Protection) Policy
- Online Safety Policy
- Use of Artificial Intelligence Policy

Policy Owner:	Head of Computer Services
Last Reviewed:	January 2024
Date of Next Review:	Academic Year 2025-26