Document No. 47.2

ICT CODE OF CONDUCT FOR STAFF

This document which applies to the whole college inclusive of boarding is publicly available on the college website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the College Office.

Scope: All who work, volunteer or supply services to our college have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal college hours, including activities away from college. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the Policies Register.

Legal Status: Complies with The Education (Independent School Standards) (England) Regulations currently in force.

Monitoring and Review: This document will be subject to continuous monitoring, refinement and audit by the Principal. There is a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. It is also updated in the interim, as may be required, to ensure that it continually addresses the risks to which students are or may be exposed. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed policy which will be made available to them in either in writing or electronically.

Reviewed: February 2026
Next Review: February 2027

Signed

David Game	John Dalton
Founder	Principal

Scope: This code of conduct should be read by all staff (including volunteers and self-employed staff) alongside the Online Safety Policy, the Safeguarding Policy, Staff Behaviour Policy and the Data Protection Policy. This code of conduct applies to any school data/information held digitally, the DGC infrastructure, desk telephones, hardware and software, photocopiers, scanners, printers, projectors and cameras.

The underlying principle of this code of conduct is that, in carrying out their roles at DGC, staff must be aware of and adhere to the laws of this country, their employment terms and conditions, their professional code(s) of conduct, where applicable, current data laws (including DGC's Data Protection Policy and the Privacy Notice) all school policies, procedures and operational guidance. Any breaches of this code must be reported to the Leadership Team and specifically to the Designated Safeguarding Lead (DSL) if it has any safeguarding aspects.

All members of staff are expected to be aware of the guidelines and policies on ICT use within DGC, and of the requirements of GDPR. Contravention of the code or guidelines may result in disciplinary action being taken against you and a serious breach could lead to dismissal. This policy supports compliance with ISSR parts 3, 6 & 7.

- Please use the ICT equipment carefully and responsibly and keep computer areas free from food and drink.
- In accordance with GDPR, (May 2018) users logged on should never leave the computer unattended without at least locking the screen. Failure to do this may result in accounts being disabled or removed.
- DGC makes use of technology to assist in our teaching and pastoral care. Staff must never project any sensitive information up onto a classroom screen. Due care must be taken when using the projector in class that such sensitive information is not inadvertently shared.
- Staff must only login to school email or use the specific safeguarding or boarding apps on any personal device (phone, laptop or tablet), if they can do so using the secure login. This device should never be left logged on and unattended.
- Staff have personal login details for IT resources that are relevant to their role. A member of staff should never use another

person's login details, nor should they, under any circumstances, share any of their personal login details with any other person, including colleagues. If a member of staff thinks that their login details might be compromised they should immediately contact IT and request that their login password(s) are reset. You should not tell your password to another person or ask for theirs.

- Files, including internet sites visited and emails stored within your user-space, can be stored by the college and may be viewed by management if necessary.
- You should not communicate with students using your personal email address or phone number, nor liaise with them on non-school matters or on social networking websites (See Online Safety Policy)
- You must not use computers to look at or produce material that would be offensive to anybody else. Take care and think before you write emails.
- If you see or receive any material that is offensive or inappropriate, please report this to the IT department.
- You must not reproduce material that might be covered by copyright rules, such as scanning books or periodicals.
- Do not allow people from outside DGC to use a school computer without permission from IT Support.
- You must prevent viruses reaching the school system by using virus checking software on your home computers. Please inform IT if you suspect a virus is within the system.
- Any emailed requests for help from the ICT department should go to support@davidgamecollege.com and not directly to individuals.
- School equipment may be borrowed only if the appropriate permission has been given by IT.
- School computers must not be used to gain illegal access to other computers or software; this is a criminal offence.
- You must not attempt to alter any computer equipment or software without permission.
- If you find equipment broken, please report this to the IT Technician.
- You must not use any computer at home or at school to publish incorrect or misleading information about the school, the school staff or governors, students or parents.
- You must not bring the school into disrepute by use of any computer system, at home or in school, including the Internet.
- If you are in doubt about how to use equipment correctly, an appropriate member of staff should be consulted.

Internet: DGC provides digital and electronic resources including an internet supply which is appropriately monitored and filtered for use by the college community. At times this provision, owing to circumstances inside or outside of the control of DGC, may be interrupted. The IT team will work appropriately to restore the required service. At such times we ask staff to use, where possible, non-digital methods of working to deliver their role to the best of their ability.

Photographs: Staff should refer to the Online Safety Policy and the Safeguarding Policy in relation to taking photographs of students. Staff should be aware that there are some parents who have refused to consent for their child to be photographed or videoed. This list of students is shared with all staff.

Staff can only take images and videos in the course of their professional duties. In doing so, they should always endeavour to use school equipment. If this is not practicable, then they may use their own personal devices. If images or videos are taken on a personal device, then all and any images must be transferred to school equipment as soon as possible. In practice this means that the images or video should be transferred to a school device on the day that the staff member returns from a trip, or, during term time, on the same day as the image or video was taken. When the image or video is transferred to a school device, it must immediately be deleted from the member of staff's personal device. No staff member should ever keep images or videos of students on their own devices.

Departmental computers: For any standalone computer equipment that is 'owned' by a particular department, for example laptops or tablets, it is the responsibility of the individuals using the equipment and ultimately the Head of Department to store the equipment safely and out of sight.

It is the job of HoDs or anyone with responsibility for any computer equipment to make sure that their computer equipment is regularly checked for viruses. All computers that connect to the school network are checked and updated whenever the computer connects to the network. Appropriate action should be taken if a virus is found. This should include informing staff if there is **any possibility** of a virus being passed from one computer to another, inside or outside the school.

Also, HODs should make sure that all equipment is used and maintained properly. All portable devices (laptops, tablets, etc) in school have access to the school network so all data must be stored and accessed from a secure and backed up school drive. School data should never be stored on these devices.

The IT staff are responsible for supporting systems throughout the College. Inevitably there will be conflicting calls upon their time and staff are asked to respect the necessary prioritising decisions which have to be made.

It is the responsibility of members of staff to ensure that their software is suitable for class use and is installed on all machines in good time by a member of the IT staff (normally a *minimum* of 5 working days is required for installation and testing). All software must be properly licensed and only installed by IT Support.

All teaching staff using computer equipment with a class should make it clear to their students that they should **never** bring and consume food or drink in the computer rooms. **All staff must reinforce this.** They should also ensure that equipment is properly used and the room is left tidy. Bags should not be stored around the computers.

Equipment on loan: Staff issued with a school device, eg. mobile phone, laptop, should use it for school business only. Occasional personal use may be necessary for appropriate reasons. In all circumstances the user of the device and the login must be the school employee issued with the device. Staff must seek to ensure that software on portable school-owned devices is current and up-to-date at all times. Staff should take notice of any update messages displayed on portable devices and apply all updates as soon as is practically possible.

Viruses: Most computers in DGC are connected to a network, and all users are asked to ensure that any disks or USB device (memory sticks) that they bring to school are checked to be clear of viruses. This includes disks that are marked 'guaranteed 100% virus free' and free CDs from magazines, or demonstration copies. The IT department must be informed immediately of any possible virus problems, or any breaches of security or other matters that might compromise the school systems. All computers should have an appropriate and up-to-date anti-virus program on and this should be used at all times.

Staff are asked not to use any disk or USB from an unknown or questionable source, since a virus could cause a great deal of inconvenience or more for all users. Viruses can be transmitted even within the school from non-networked machines to networked machines on a USB device (memory stick). Staff should be suspicious of any documents emailed from an unknown source, as these could be a problem. These should be deleted and not opened. If in doubt, please consult IT support.

Members of staff are not permitted to install any software on networked machines without prior consultation with the IT Department. Nor must they allow students to do so.

Whilst it is clear from the above that DGC will take all reasonable precautions against invasion by a virus, the school can accept no responsibility or liability if a virus is transmitted to external computers from school computers, or if school work is affected by a virus on a school computer from an external or internal source.

Passwords: Passwords are used to protect the data on our system. Some programs require the use of passwords, in addition to logging on to the system at the start. The data held in the school information system is sensitive and confidential. Teaching staff have varying levels of access to this data depending on their role at DGC. 2-factor or 2-step authentication (sometimes called 2FA or MFA) is enabled .

- Passwords should be a minimum of 8 characters and should include at least one each of the following: upper and lower case letters, numbers and special characters
- passwords should be changed on a regular basis
- You should use a different password on every system or website you log into, unless the system uses single sign-on (SSO)
- All passwords should be securely stored. If you have to write a password down, it should be kept out of sight and should not be easily readable by another person
- You must change a password immediately if you think it might have been compromised.

Backups: All school network drives are backed up daily. If files/folders are accidentally deleted then they can only be restored to the state of the previous day.

Email: Every member of staff will be given an email address, which can be quoted in correspondence and can be used for any school-related work. We also expect staff to check their emails at least twice a day (see Email Policy).

Email Risks: The power of instantaneous, world-wide communication by email potentially poses significant risks to the School and members of the school community in relation to:

- Defamation or malicious falsehood, through the careless or vindictive composing, sending and/or distributing of gossip or messages maligning a person, a group of persons or an organisation (including the School);
- Unlawful harassment and/or discrimination on the grounds of sex, race or disability between one member of staff and another, for which the School may be vicariously liable;
- *'Electronic bullying'* between staff and/or students for which the School may be vicariously liable;
- Users forgetting or not realising that email messages can be retrieved even once deleted and may have to be disclosed in the event of subsequent litigation;
- The possibility that an unauthorised contract may be formed by a student (or a member of staff) having ostensible authority on behalf of the School;

- Interception, unintended receipt or unauthorised reading of emails by others, for example through hacking, disclosure of passwords or careless use of distribution and address lists;
- Plagiarism and/or breach of copyright by sending, receiving or using, without appropriate permission and acknowledgment, the intellectual property belonging to another;
- Revealing personal information about oneself or another (in breach of the *Data Protection Act 1998 and GDPR May 2018);*
- Transmission of viruses as email attachments.

Internet Risks: In addition to the features and dangers of simple emails, the Internet facilitates and provides other forms of electronic communication and information such as access to and use of website, newsgroups, list servers, links, games and programs. There is also the growing commercial use of the Internet to sell goods and services worldwide.

- Some of the images and text available on the Internet to view, download or attach to an email are, or may be, harmful to students and the school community as a whole, e.g. pornographic, racist, sexist, blasphemous or violent material.
- A further danger is that of importing viruses onto the School's network or passing viruses to a third party, via material downloaded from or received via the Internet (or brought into school on disk or USB).
- Some files may be very sizeable and therefore costly and time consuming to download. Large files also take up valuable memory capacity, thus having an adverse effect upon the performance of the School's computer system.

MAILINGS TO PARENTS

Any letters or information sent to parents should always be checked beforehand by a member of the LT. This is for accuracy and to ensure that we maintain a standard house style. It is also strongly advised that any 'mass mailing' by email to groups of parents is checked by a member of the SLT beforehand.