EAGLE HOUSE SCHOOL

Academic Year 2023 - 2024

Document Control

Title of Policy:	**The Wellington College ICT Acceptable Use Policy**
Policy/Procedure Owner:	Tony Whelton (Director of IT Services, Wellington College)
Date Last Reviewed:	June 2023
Ratified by Governors:	n/a

The Wellington College ICT Acceptable Use Policy

The Wellington College is a Royal Charter Body and charity registered with number 309093 (**TWC**). TWC operates two schools, Wellington College and Eagle House School, and has two wholly owned subsidiaries, Wellington College Services Ltd (which also trades as, inter alia, Wellington Health & Fitness Club) and Wellington College Educational Enterprises Ltd (which also trades as, inter alia, Wellington College International).

This policy applies to anyone who is provided with an email address by any of the organisations forming part of TWC (a **Wellington email account**) and anyone who accesses TWC's IT systems, whether through Wi-Fi or otherwise (the **Wellington IT systems**) (together, the **Wellington Community**).

This policy applies at all times that a person has access to their Wellington email account or is accessing the Wellington IT system, regardless of whether they are on a Wellington site or whether it is during term time or outside of working hours.

- This policy should be read in conjunction with the relevant safeguarding, pastoral, data protection and discipline policies as well as the Whistleblowing Policy. Staff family members should read this in conjunction with the Adults Living on Site Policy.

Online behaviour

As a member of the Wellington Community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the Wellington Community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the Wellington Community, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the Wellington IT systems

Whenever you use the Wellington IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access Wellington IT systems using your own username and password. Do not share your username or password with anyone else.

- Do not attempt to circumvent the content filters or other security measures installed on the Wellington IT systems (via Virtual Private Networks (VPN's) or other systems), and do not attempt to access parts of the system that you do not have permission to access.
- TWC monitors use of the Wellington IT systems, and can view content accessed or sent via its systems. A random sample of emails between staff and pupils are monitored on a monthly basis by the Director of IT Services and only shared with Director of Safeguarding.

Passwords

Passwords protect the TWC network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as personal passwords you may use. We encourage use of multi-factor authentication (MFA) which is best practice. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to TWC should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Services Helpdesk.

Use of TWC systems

The provision of Wellington email accounts and Wellington IT systems is in the main for official TWC business, administration and education. It is acknowledged that staff who live on site will access TWC provided Wi-Fi for personal use but they must be aware that web use is monitored on all TWC Wi-Fi. It is important that staff do not use their Wellington email accounts for personal and family purposes but have a separate private email account. Pupils should keep their personal, family and social lives separate from their Wellington IT use and limit as far as possible any personal use of these accounts. Again, please be aware of Wellington's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official Wellington business must be conducted on Wellington systems, and it is not permissible to use personal email accounts for Wellington business.

In order to access Wellington data on your personal device you will need to install Microsoft Company Portal (Intune) to ensure that the data it contains is secure in case of loss. Installing Company Portal allows the Wellington data to be protected by the IT Services Department.

The use of non-authorised Cloud storage systems for Wellington data is prohibited as all data must be maintained within the Wellington IT systems (Microsoft Office365).

Monitoring and access

All members of the Wellington community should be aware that Wellington email and internet usage (including through Wellington Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and Wellington email accounts may be accessed by Wellington where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Cyber-bullying

Cyber-bullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet to deliberately upset someone else.

TWC believes that all individuals have a right to feel safe and are protected from all forms of cyber-bullying. Examples of cyber-bullying include:

- Calls, social media posts, messages or emails, containing homophobic, racist, sexist or otherwise unpleasant language or is otherwise threatening, intimidating or harassing;
- Videoing other people being harassed and sending these to other phones or internet sites;
- Taking or sharing humiliating or inappropriate images;
- Sending nasty, threatening or anonymous messages using social media sites, chatrooms or message boards; making friends under false pretences; groups of people deciding to pick on or ignore individuals;
- Using someone else's account to forward rude or mean emails; forwarding unsuitable content including images or clips or sending computer viruses;
- Accessing another person's account details and sending messages, deleting information or making private information public.

By engaging in any of the aforementioned activities, an individual would be in breach of the College AUP. Students would also be in breach of the Child-on-child abuse policy and more details about cyber-bullying can be found in this policy. Members of staff would also be in breach of the Staff Code of Conduct. All members of the Wellington community have a right to be safe and can report any cyber-bullying (whether to themselves or others) to:

- In the case of Wellington College students: their HM, Mrs Lynch (Director of Safeguarding and Designated Safeguarding Lead), Mrs Eyers (Safeguarding Manager), Mr Wayman (Deputy Head Pastoral and Wellbeing), another member of staff or a College prefect. Students can also use the anonymous reporting tool, Whisper;
- In the case of Eagle House pupils: Mrs Goves (Deputy Head, Safeguarding);
- In the case of members of staff: to their line manager, the DSL or the HR department;
- In the case of staff family members living on site, the DSL;
- For visitors: to Security staff or the DSL.

Wellington College has the right to take action against an individual if that individual is involved in incidents of inappropriate behaviour, that are covered in this agreement, when the out of College and where they involve membership of the College community.

Any individuals failing to comply with this Acceptable Use Policy Agreement, will be subject to disciplinary action. For pupils and staff, the disciplinary action will be in accordance with the relevant disciplinary policy and the appropriate sanction applied. For other members of the Wellington community, an investigation will be carried out if, in the opinion of TWC (acting reasonably) the circumstances allow and a sanction applied. In other circumstances, TWC may decide to remove a person's access rights without conducting an investigation. For all members of the Wellington community, it may be appropriate to suspend access to their Wellington email or Wellington IT systems whilst any investigation is being conducted. If an individual behaves irresponsibly, they may also be denied full access to the College ICT facilities and that the College will act strongly against anyone whose use of ICT risks bringing Wellington College into disrepute. Where misuse of a Wellington email or the Wellington IT systems by any member of the Wellington community appears to be illegal, TWC shall inform the Police and may be obliged to suspend any internal investigation

whilst a Police investigation is on-going. In the case of pupils, their parents may be informed; in the case of family members living on site, the relevant member of staff shall be informed.

Reporting

Members of the Wellington community should report the following online safeguarding concerns immediately to a member of the Safeguarding Team:

- Witnessing or suspecting unsuitable material has been accessed
- Being able to access unsuitable material
- If teaching topics which could create unusual activity on the filtering logs
- There is failure in the software or abuse of the system
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- Noticing abbreviations or misspellings that allow access to restricted material

Breach reporting

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. Any breach of personal data by any member of the Wellington Community must be reported immediately to the Data Office (data@wellingtoncollege.org.uk) and, in the case of pupils, your HM. Failure to promptly report a data breach may result in disciplinary action.

Data breaches will include almost any loss of, or compromise to, personal data held by Wellington regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the Wellington IT systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

Wellington must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, Wellington must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

Data breaches will happen to all organisations, but Wellington must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all members of the Wellington community. Wellington's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Reviewed TJW, DAL and KEJB June 2023