wqe | Wyggeston &
Queen Elizabeth I
College

Acceptable Use Policy

<table>
<tr><td>Policy Name</td><td colspan="4">Acceptable Use Policy</td></tr>
<tr><td>Responsible Senior Leader</td><td colspan="4">Associate Principal – Learning and People Strategy</td></tr>
<tr><td>Policy Owner</td><td colspan="4">IT Services Manager</td></tr>
<tr><td>Approved By</td><td colspan="4">ELT, CSLG, SBSLG</td></tr>
<tr><td>Approval Date</td><td colspan="4">June 2025</td></tr>
<tr><td>Next Approval Date</td><td colspan="4">June 2026</td></tr>
<tr><td rowspan="2">Intended Audience</td><td>Students</td><td>Staff</td><td>Governors</td><td>External</td></tr>
<tr><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Published to Staff Intranet</td><td colspan="2">Yes</td><td colspan="2">As Titled</td></tr>
<tr><td>Published to Student Intranet</td><td colspan="2">Yes</td><td colspan="2">As Titled</td></tr>
</table>

Amendment Summary

Version	**Date**	**Comments**
1.0	12/06/2024	First draft of reviewed policy.
1.1	25/06/2024	Numbered. DP Act is now 2018; the 1998 one superseded. Added 5.4 use of college email address for personal business.
1.2	14.08.2025	Page 3 – Inserted new section – 6 Use of Artificial Intelligence (AI)

Acceptable Use Policy

The college is committed to the equality of opportunity and to a proactive approach to equality, which supports and encourages under-represented groups, promotes inclusivity and values diversity.

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to enable WQE College to –

1.1. Ensure its IT facilities are used lawfully; safely; reasonably; and in a manner that raises no unnecessary risks or security threats to the college.

1.2. Ensure it meets its obligations with regards to the Janet Acceptable Use Policy and the Janet Security Policy.

1.3. Provide a framework to facilitate the proper and extensive use of Information Technology (IT) in the interests of learning, teaching, including business and community engagement partnerships.

2. Scope

This policy applies to –

2.1. Anyone using college IT facilities including, but not limited to, students, staff, sub-contractors, and governors.

2.2. All use of college IT facilities regardless of the ownership of devices being used for access, e.g., college owned devices, personally owned devices, and devices belonging to third parties.

3. Responsibilities

3.1. It is the responsibility of all users of college IT facilities to read, understand, and comply with this policy and any relevant policies related to their IT activities.

3.2. All users must comply with any reasonable written or verbal instructions issued by IT Services in support of this policy.

3.3. An end-user accepts that there is no expectation of privacy when using college IT facilities and understands that members of IT Services have full access to all data and materials in all systems.

3.4. Whilst the college takes appropriate security measures against the unauthorised access to, alteration, disclosure, destruction, or accidental loss of an end-user's files, it cannot and does not give any guarantees about security, confidentiality, or integrity of data and files.

3.5. Contravening this or any other related policy can lead to disciplinary action being taken.

3.6. The use of college IT systems means agreement with this Acceptable Use Policy and related policies.

4. Credentials, Authentication, and Identity

As an end-user of college IT facilities, you must –

4.1. Take all precautions to safeguard your passwords and any other IT credentials issued to you.

4.2. Only use the access provided to college IT facilities for which the purpose was granted.

4.3. Not disclose your passwords to anyone, including IT staff.

4.4. Not allow anyone else to know or use your IT credentials.

4.5. Not attempt to obtain or use anyone else's IT credentials.

4.6. Not leave unattended a computer that you are logged onto to.

5. Acceptable Use

5.1. All use of college IT facilities must adhere to all relevant license conditions when using software procured by the college.

5.2. A reasonable level of personal use of college IT facilities is permitted, but it must not interfere with college business, the performance of college duties, or expose the college to additional risk.

5.3. Personal use of college IT facilities is a privilege that may be withdrawn by the college at any point if such use is not in accordance with this policy.

5.4. Your college email address should not be used for personal business unless necessary, for example when an academic email address is required. Using the college email address for personal business adds risk to the college and to yourself.

6. Use of Artificial Intelligence (AI)

The college recognises the growing role of Artificial Intelligence (AI) tools in education, administration, and personal productivity. All use of AI tools and services must adhere to the following principles:

6.1. AI tools must be used in ways that support learning, teaching, and college operations, and must not undermine academic integrity or professional standards.

6.2. Users must not use AI to generate or disseminate misleading, harmful, discriminatory, or offensive content.

6.3. AI-generated content must be clearly identified where appropriate, especially in academic or professional contexts.

6.4. Users must not input confidential, personal, or sensitive college data into public or third-party AI tools without explicit authorisation.

6.5. The use of AI must comply with all relevant college policies, including data protection, safeguarding, and copyright.

6.6. Staff and students are encouraged to seek guidance from IT Services or Learning & People Strategy teams when unsure about appropriate AI use.

7. Behaviour

7.1. The conduct of end-users of college IT facilities should always be in line with student and staff codes of conduct and respect the college's values.

7.2. In addition, the college has a statutory duty under section 26(1) of the Counter-Terrorism and Security Act 2015, known as the Prevent Duty, to have due regard to and aid the process of preventing people from being drawn into and supporting terrorism. It is part of the Government counter-terrorism strategy with the aim of reducing the threat to the UK.

When using college IT facilities, you must not –

7.3. Create, download, store, or transmit extremism related material with the intention of supporting or spreading terrorism. The college reserves the right to monitor, or block access to such material.

7.4. Undertake any illegal activity or use the IT facilities in a way that interferes with others valid use of them.

7.5. Create, download, store, or transmit unlawful material; material that is indecent, offensive, threatening, or discriminatory.

7.6. Create, transmit, or display material that deliberately and unlawfully discriminates, or encourages deliberate or unlawful discrimination, on the grounds of race, ethnicity, gender, sexual orientation, marital status, age, disability, political or religious beliefs.

7.7. Create, transmit, or display defamatory material.

7.8. Obtain, transmit or store materials where this would breach the intellectual property rights or copyright of another party. This includes downloading and sharing music, video, and image files without proper authority.

7.9. Download, copy or share any personal data belonging to other users, including their photograph.

7.10. Create or transmit material with the intent to defraud.

7.11. Access or attempt to access, college systems and information for which permission has not been granted.

7.12. Share information for which the college is responsible when not authorised to do so.

7.13. Intentionally interfere with the normal operation of the IT network. For example, spreading malware or viruses; or undertaking activity causing sustained high volume network traffic that hinders others in their use of the IT network.

7.14. Undertake any activity that jeopardises the security, integrity, performance, or reliability of electronic devices, computer equipment, software, data, and other stored information. This includes the unauthorised monitoring or interception of network traffic.

7.15. Attempt to disrupt or circumvent IT security measures by any means.

7.16. Participate in any other activity that could bring the college into disrepute.

8. Monitoring

The college records and monitors the direct and indirect use of IT facilities for various purposes including:

8.1. Security: detecting, preventing, and investigating inappropriate access to, or use of, IT systems or data.

8.2. Operational: fault investigations; performance and capacity planning; and service upgrades.

8.3. Compliance: checks against college polices and regulatory requirements.

8.4. Law: requests or requirements for information from law enforcement agencies.

8.5. This applies to all devices whether college owned, personally owned, or owned by a third-party, that are used to access the internet and world-wide-web, noting that your devices may, due to being connected to the college wireless network, pass data through the college's network to and from the internet, even when the devices are not being actively used.

9. Legislation

The use of college IT facilities is bound by UK laws. The following is an illustrative list of applicable UK laws, the Data Protection Act 2018, the Copyright, Designs and Patents Act 1988, the Protection from Harassment Act 1997, the Communication Act 2003, the Malicious Communications Act 1988, the Public Order Act 1986, the Obscene Publications Act 1959 and 1964, the Protection of Children Act 1978, the Sexual Offences Act 2003, the Computer Misuse Act 1990, the Counter Terrorism and Security Act 2015.

= = = END = = =