

Information Technology: Acceptable Use Policy

1. Introduction

- 1.1 The IT systems provided for use by all users (staff, students, apprentices, contractors and authorised visitors) are the property of Walbrook and their use is made available for the purposes of learning, research and administration. This document sets out the ground rules for the use of these systems. It applies to all users and roles and is intended to protect Walbrook and its students, and staff.
- 1.2 Please read this document and be sure that you understand it, as you will be expected to abide by these rules.

2. Scope

- 2.1 This policy applies to all IT systems and equipment made available by Walbrook, including the network and all directly or indirectly connected systems, and services provided off-site by third parties contracted to do so. It also applies to the production of any material using institutional facilities, including printed output, web pages, emails, social media platforms, bulletin boards, blogs, forums and any other online channels.
- 2.2 This policy also applies to personal devices (including smartphones, tablets and laptops) used to access Walbrook systems, networks or data, whether on Walbrook premises or remotely. Users accessing Walbrook systems from personal devices must ensure those devices have up-to-date security software installed.
- 2.3 References to 'IT systems' and 'IT facilities' in this policy include cloud-based services, collaborative tools, virtual learning environments, video-conferencing platforms, social media and artificial intelligence (AI) tools accessed through or in connection with Walbrook systems or for institutional purposes.
- 2.4 Throughout this policy, all references to students shall include apprentices.

3. Use of Walbrook IT Systems

- 3.1 You must adhere to the conditions laid down by the Jisc Acceptable Use Policy.
- 3.2 You must show consideration for other computer users at all times.
- 3.3 You are responsible for keeping your password secure and reasonable precautions must be taken to minimise the risk of unauthorised access.
- 3.4 Personal use of email and Internet services may be logged and these logs may be used to ensure compliance with UK legislation, including the Prevent duty, to detect or investigate unauthorised use of systems, to prevent crime or in the interests of national security.
- 3.5 Use of social media for personal purposes during work or study time must not interfere with your responsibilities to Walbrook. Where you identify yourself as being connected with Walbrook in any social media context, you must ensure your conduct reflects the standards set out in this policy and in Walbrook's other relevant policies.
- 3.6 AI tools and generative AI platforms may be used for learning, research and administrative purposes subject to any guidance issued by Walbrook. You must not input personal data, confidential institutional information, or safeguarding-sensitive material into AI tools without authorisation. The Academic Integrity Policy and the Generative AI Usage Policy apply alongside this policy.

4. Unacceptable Use

- 4.1 Walbrook has a statutory duty under the Counter-Terrorism and Security Act 2015, termed "Prevent". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. Walbrook also has safeguarding duties under the Children Act 1989 and 2004, and has regard to Keeping Children Safe in Education insofar as applicable to its provision, both of which extend to online environments.
- 4.2 You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Walbrook reserves the right to block or monitor access to such material.
- 4.3 You must not access, or attempt to access, any computer material or system for which access authorisation has not been given.
- 4.4 You must comply with the terms and conditions of all licence agreements relating to software and data networks.
- 4.5 You must not send or forward junk or chain email and not use email for the mass distribution of unauthorised and unsolicited messages.
- 4.6 You must not deliberately introduce, or risk introducing, any virus or other harmful software, nor take any action to circumvent any anti-virus precautions established by the IT department.
- 4.7 You are required to respect the copyright of all materials and software made available for your use.
- 4.8 You must not load any software onto the IT facilities provided without permission from the IT department. The IT department has the right to remove any software installed without permission.
- 4.9 Files containing data about living individuals must not be constructed or maintained without ensuring compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. All personal data processed using Walbrook IT systems must be handled in accordance with Walbrook's Data Protection Policy.
- 4.10 You must not use the IT facilities in a way that denies service to other users, for example, deliberate or careless overloading.
- 4.11 You must not damage any of the IT facilities or any accommodation or services associated with them.
- 4.12 You must not use AI tools or generative AI platforms to create, adapt or distribute material that is discriminatory, extremist, harmful, unlawful, or intended to harass or deceive others. You must not use AI tools to circumvent academic integrity requirements or in any way not permitted under Walbrook's Academic Integrity Policy or the Generative AI Usage Policy.

5. Online Safety and Prevent

- 5.1 Walbrook maintains web content filtering controls to restrict access to categories of material that are unlawful, extremist, harmful or otherwise contrary to this policy. The Prevent Lead (Chief Governance Officer) is responsible for liaising with the relevant technical services lead to ensure that filtering controls are appropriate, maintained and reviewed at least annually. The scope, categories and effectiveness of filtering are reported to the Safeguarding and Prevent Group.
- 5.2 Any user who encounters material through Walbrook IT systems that suggests a risk of harm, radicalisation, child sexual abuse, domestic abuse, or any other safeguarding concern must report it promptly as follows in clauses 5.3, 5.4 and 5.5 below.

- 5.3 Safeguarding concerns (including child protection, abuse or self-harm): report to the Designated Safeguarding Lead (DSL) at safeguarding@walbrook.ac.uk or by the contact details set out in the Safeguarding Policy.
- 5.4 Concerns relating to radicalisation or terrorism should be reported promptly through safeguarding@walbrook.ac.uk, marked for the Prevent Lead.
- 5.5 Where there is an immediate risk of serious harm, contact the emergency services (999) in the first instance and notify the DSL and Prevent Lead as soon as practicable.
- 5.6 Potential indicators of online radicalisation may include, but are not limited to: engaging with or disseminating extremist, terrorist, or far-right/far-left violent material; expressing endorsement of proscribed organisations; interacting with individuals who advocate violent extremism; or exhibiting notable changes in online behaviour or language. Staff and students who identify such indicators in themselves or others should report these through safeguarding@walbrook.ac.uk, marked for the Prevent Lead, without delay, as set out in clause 5.4.
- 5.7 Online conduct is governed by the same standards as face-to-face conduct. Walbrook's Safeguarding Policy, Prevent Policy, Equality and Diversity Policy and Student Code of Conduct apply to all online activity conducted through Walbrook systems or in a Walbrook context, including on social media.

6. Roles, Responsibilities and Review

- 6.1 The Head of IT Security and Compliance and the Head of IT Technical Services own this policy and are responsible for ensuring that it is kept up to date and aligned with Walbrook's wider safeguarding, Prevent, data protection and information security arrangements. The Designated Safeguarding Lead and Prevent Lead should be consulted on any material changes to sections concerning online safety, monitoring, reporting, escalation or risk indicators.
- 6.2 This policy is reviewed annually. Amendments are scrutinised by the Safeguarding and Prevent Group, which recommends them to SLG, after which they proceed through LTQC and Academic Board to the Board of Directors for approval.

7. Law

- 7.1 It is the responsibility of all users to comply with all applicable UK legislation, including (but not limited to):
- Computer Misuse Act 1990
 - Copyright, Designs and Patents Act 1988
 - Counter-Terrorism and Security Act 2015
 - Criminal Justice and Public Order Act 1994
 - General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
 - Regulation of Investigatory Powers Act 2000
 - Equality Act 2010
 - Online Safety Act 2023
 - Children Act 1989
 - Children Act 2004
 - Education Act 2002
 - Education and Training (Welfare of Children) Act 2021, insofar as applicable
 - Working Together to Safeguard Children
 - Keeping Children Safe in Education (insofar as applicable)
 - Modern Slavery Act 2015

- Serious Crime Act 2015

8. Liability

- 8.1 Whilst Walbrook takes appropriate security measures to protect data and software, it cannot accept responsibility for the loss of any data or software or the failure of any security or privacy mechanism.
- 8.2 Walbrook accepts no responsibility for the malfunctioning of any computing hardware, software or facility.
- 8.3 No claim shall be made against Walbrook, its employees or agents in respect of any loss, damage or inconvenience alleged to have been caused whether by defect in the resources or by act or neglect of Walbrook, its employees or agents.
- 8.4 Nothing in this policy excludes or limits liability for death or personal injury caused by negligence, for fraud or fraudulent misrepresentation, or for any other liability that cannot lawfully be excluded or limited, including under the Consumer Rights Act 2015.

9. Failure to Abide by the Rules

- 9.1 Infringement of these rules may be subject to penalties under civil or criminal law and Walbrook is prepared to invoke such law and liaise with the relevant legal authorities.
- 9.2 Infringement of these rules may constitute a disciplinary offence and, regardless of legal proceedings, established disciplinary procedures will be followed.
- 9.3 Concerns or suspected infringements relating to safeguarding or the Prevent duty should be reported in accordance with Section 5 of this policy and with Walbrook's Safeguarding Policy and Prevent Policy, copies of which are available on the Walbrook website and the VLE.

10. Related Policies and Guidance

- Safeguarding Policy
- Prevent Policy
- Data Protection Policy
- Equality and Diversity Policy
- Academic Integrity Policy
- Generative AI Usage Policy
- Staff Code of Conduct
- Student Code of Conduct
- Visiting Speaker Policy
- Freedom of Speech Code of Practice
- Disciplinary procedures and relevant complaints procedures

11. Document Control

Version	2.4
Approved by	Board of Directors [pending]
Approval route	Safeguarding and Prevent Group → Senior Leadership Group (SLG) → Learning, Teaching and Quality Committee (LTQC) → Academic Board → Board of Directors
Author	Provost
Owner	Head of IT Security and Compliance and Head of IT Technical Services
Date approved	[13 October 2026]
Implementation date	23 October 2026 [pending approval]
Review date	Autumn 2027