IT Acceptable Use Policy

Policy no:	6.9
Version no.	24.11
Author:	IT Manager
Next review due:	September 2025
Last review date:	November 2024
Responsible Board:	Corporate and Planning Board
Approved by & date:	September 2024
Linked policies and documents:	Data Protection Policy Policy on Rights in Relations to Your Data Student Privacy Policy
External references:	Data Protection Act 2018 General Data Protection Law Counter-Terrorism and Security Act 2015
	UK Quality Code UKSCQA/02 Advice and Guidance on Monitoring and Evaluation (6.7) *Providers take account of ethics and data protection requirements when designing and operating monitoring and evaluation systems.*
	ICO No. Z1097339
	optindigo.com for GDPR Consultancy and Support
Audience:	External

Table of Contents

1 Introduction

Oxford Business College (OBC) recognises the integral role that Information Technology (IT) plays in the academic and administrative functions of the institution. As such, it is imperative to establish clear guidelines and standards for the responsible and effective use of IT resources by all members of the OBC community. This IT Usage Policy outlines the expectations, responsibilities, and procedures governing the use of OBC's IT infrastructure, equipment, and systems.

2 Purpose

The purpose of this policy is to ensure the secure, ethical, and efficient utilisation of IT resources across OBC. By providing clear guidelines and expectations, this policy aims to safeguard the institution, its data, and its community members from potential risks and threats associated with improper IT usage. Additionally, this policy serves to promote a culture of accountability, professionalism, and compliance with legal and regulatory requirements regarding IT usage.

3 Aims & Objectives

The principal aims and objectives of the OBC IT Usage Policy are as follows:

3.1 To establish clear guidelines and standards for the responsible and ethical use of IT resources by all members of the OBC community.

3.2 To safeguard the institution, its data, and its community members from potential risks such as data loss, identity theft, and other digital and physical threats.

3.3 To promote a culture of accountability, professionalism, and compliance with legal and regulatory requirements regarding IT usage.

3.4 To facilitate the effective and efficient utilisation of IT resources in furthering the mission and objectives of OBC, including academic and administrative functions.

3.5 To provide guidance and support to users regarding the proper management, security, and protection of data and information accessed or stored using OBC's IT infrastructure, equipment, and systems.

4 Scope

This policy applies to all employees, students, and partners of OBC, including visiting lecturers, board members, and guests/guest speakers.

Oversight and enforcement of this policy are the responsibility of the Chief Operating Officer and Chief Financial Officer, in collaboration with key partners and stakeholders.

Any breaches of this policy shall be addressed in accordance with the relevant Student Code of Conduct and Student Disciplinary Policy or Disciplinary & Staff Grievance Policy.

5 Acceptable Use

All usage of IT equipment and systems must align with furthering the mission and objectives of OBC and should be conducted in a safe and responsible manner.

All IT equipment and infrastructure remain the property of OBC and may be monitored, reviewed, and disclosed to uphold their appropriate use.

Devices and software must not be altered, installed, or otherwise modified unless authorised by a member of the IT team.

Interactions via email, Microsoft Teams, and other digital platforms should adhere to OBC's values as delineated in the Student Code of Conduct and Student Disciplinary Policy, Disciplinary & Staff Grievance Policy, Communications policy, and the Staff Handbook.

6 General Principals

The College provides IT facilities primarily for business and academic reasons and for the conduct of legitimate College business, not for the purposes of entertainment, shopping or other private use.

Users must treat information that they access or see via the College's IT systems as confidential, unless the information is clearly intended to be public or disclosable in the context in which it is made available.

Users must contact the College's IT Services department for any change or modification to hardware and software; any such change should be made only by authorised members of the College's staff.

Users are required to respect the legitimate access to the IT facilities by other users and must not obstruct this or remove or interfere with output created by any other user.

Users must be considerate when using the College's IT facilities, including keeping noise to a minimum and keeping behaviour appropriate to an academic or business setting; in other words, conduct should be quiet and orderly.

Although the College's IT facilities are provided primarily for legitimate academic and business purposes, the College permits limited personal use of email and of the internet subject to the rules set out in this policy and provided that such use does not conflict with the College's interests, such as the proper performance by staff of their work for the College.

Access to another person's emails will only be granted with the explicit consent of the College's Managing Director

6.1 Data Protection

OneDrive, to ensure proper management and access control.

Microsoft Teams should be utilised for shared documents and collaboration, while OneDrive should be used to limit access to individual users.

USB external drives are strictly prohibited for storing data; only OBC-based cloud storage

solutions outlined above should be used.

Sharing of files and data should be limited to necessary personnel and conducted through secure methods such as Teams or OneDrive links.

For further guidance on Data Protection, employees should refer to the Data Protection Policy.

6.2 Devices and Equipment

6.2.1 All data and sensitive information must be securely stored and protected from unauthorised access and loss.

6.2.2 Passwords and accounts must be kept confidential and meet established security standards, such as minimum length requirements.

6.2.3 Data and files should only be stored in designated locations, namely SharePoint, Microsoft Teams and Devices and Equipment

6.2.4 Devices and equipment provided by OBC remain the property of the institution and must be safeguarded against loss and damage.

6.2.5 Any defects or damage to equipment should be reported to the IT team promptly, and repair should only be attempted by authorised personnel.

6.2.6 OBC-owned equipment should only be used for tasks related to supporting the college's goals and not for personal use.

6.2.7 Staff should use only the devices issued to them for OBC work and refrain from using personal devices for work purposes.

6.2.8 In cases where OBC has not issued devices to staff members, any personal devices used for OBC work should be treated with the same level of security and subject to potential audits by the institution.

6.2.9 Devices must be securely stored when not in use and should not be shared with other members of the OBC community or third parties to prevent unauthorised access and potential security breaches.

7 Prohibitions and restrictions

7.1 Password and identity integrity

7.1.1 Revealing any account password (or associated secret authentication information) to others or allowing use by another person, including family and other household members.

7.1.2 Circumventing user authentication or security of any host, network service or account. Impersonating another user.

7.2 Hacking and similar misuse

7.2.1 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's network session, via any means, locally or via the Internet/Intranet/Extranet.

7.2.2 Gaining unauthorised access to, or intentionally damaging, other computer systems,

network services or the information contained within them, this includes erasing, altering, corrupting or tampering with any information other than in the legitimate conduct either of College business for staff or for the proper furtherance of academic study for students.

7.2.3 Executing any form of network monitoring that will intercept data not intended for the user's host.

7.2.4 Port scanning or security scanning unless being conducted by authorised members of the College's IT Team (or third parties specifically authorised by IT Team.)

7.2.5 Introducing malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs etc)

7.2.6 Effecting security breaches or disruptions of network communication. Examples of security breaches are accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

7.3 Illegality

Any unlawful activity not otherwise covered. Examples of such unlawful activity include:

7.3.1 Infringement of intellectual property rights including distributing or obtaining illegally copied software, media or other material.

7.3.2 Breaching another person's privacy.

7.3.3 Harassment or bullying.

7.3.4 Defamation.

7.3.5 Sending unsolicited advertising or promotional material.

7.3.6 Conducting any corrupt practice.

7.3.7 Fraud.

7.3.8 Theft.

7.3.9 Gambling.

The creation, transmission, storage, downloading or display of any offensive, obscene, discriminatory (either on the grounds of sex, disability, colour, race, religion or belief, or sexual orientation), indecent, explicit or threatening data or other material, unless such access is necessary for one or more of the reasons below:

7.3.10 Authorised research activity

7.3.11 Investigatory or disciplinary process

7.3.12 Whistleblowing

7.3.13 Cooperation with the Police, Prevent or other official enquiry.

Users should be aware that the College takes its responsibility under the Counter-Terrorism and Security Act 2015 extremely seriously including those requirements detailed in Section 29 of the Act and referred to as the "Prevent Duty". Consequently, users must not deliberately

create, display, produce, store, circulate or transmit material related to terrorism or extremist ideology in any form or medium except where required as set out for the necessary reasons above.

Users shall not use the College's IT or network facilities for any of the following (the titles are prompts to assist reference only):

7.4 Confidentiality including email forwards

7.4.1 Disclosing any information about, or providing lists of, College staff or students to any party not employed by the College (unless in the course of legitimate College business or authorised by a member of the senior management of the College.)

7.4.2 Storing any confidential information on any system other than those provided by the College, unless formally approved by the College's IT team.

7.4.3 Sending any confidential information online by any means, without utilising appropriate, approved, security methods. Online communications may be subject to interception by persons outside the College and such interception may not be detectable or perceptible by the user. Any encryption software used should be provided by or approved by the College's IT Team.

7.4.4 Using an automatic forwarding facility for email which takes email from a College account to an outside network unless, in the case of staff, this has been approved by an appropriate manager. Automatic email forwarding may result in the inadvertent transmission of sensitive information to external email accounts and users should therefore exercise utmost caution when sending any email from a College account to an outside network.

7.5 Miscellaneous prohibitions

7.5.1 Private profit, except to any extent authorised in writing under a user's conditions of employment or other express agreement with the College.

7.5.2 Connecting any unsecured device to the College's IT systems without prior consent.

7.5.3 Failing to read or adhere to the terms and conditions of any licence agreements relating to the relevant IT facilities including software, equipment, consumables, services, databases, platforms, publications and goods.

8 Remote Working

If working or studying remotely, individuals must ensure that their working environment meets safety standards, both digitally and physically.

Wi-Fi networks used for remote work should be secure and private, and individuals should avoid using open networks, such as those in public places like coffee shops or bars.

Electrical components such as chargers and plugs must be regularly checked for any signs of damage or wear, and only chargers issued by OBC should be used with devices to ensure safety and compatibility.