St John's College
Oxford

Name of Regulation: College Regulations Relating to the Use of Information Technology Facilities

RESPONSIBLE COMMITTEE: Academic Services
RESPONSIBLE OFFICER: Principal Bursar
LINKED DOCUMENTS: College: IT Policy; Rules for Network Access in the College; Information Security Policy; Social Media Policy, Data Protection Policy.
LINKED DOCUMENTS: Other: University regulations relating to the use of Information Technology Facilities; University mobile/wireless rules.
Annual Review date: First meeting in Hilary Term

1. Purpose of this policy is to detail the regulations concerning the use of information technology facilities in the College.

2. This policy should be read together with the University's Statues and Regulations in this area https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002

3. College IT and network facilities are provided for use in accordance with the following policy set by Governing Body:

(a) Users are not permitted to use College IT or network facilities for any of the following: activities not directly connected with employment, study, or research in the University or the colleges (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation.

(b) Individuals have no right to use College facilities for any other purpose.

4. The College reserves the right to exercise control over all activities employing its computer facilities, including examining the content of users' data, such as e-mail, where that is necessary:

(*a*) for the proper regulation of the College's facilities;

(b) in connection with properly authorised investigations in relation to breaches or alleged breaches of provisions in the College's statutes and regulations, including these regulations; or

(*c*) to meet legal requirements or otherwise in the context of legal proceedings or the taking of legal advice, in accordance with such procedures as may be approved by Governing Body for this purpose.

(*d*) Such action will be undertaken only in accordance with these regulations.

5. These regulations govern all use of College IT and network facilities, whether accessed on College property or otherwise.

6. Use is subject at all times to such monitoring as may be necessary for the proper management of the network, or as may be specifically authorised in accordance with these regulations.

7. Persons may make use of College facilities only with proper authorisation.

   (*a*) 'Proper authorisation' in this context means prior authorisation by the appropriate officer, who shall be the IT Manager or his or her nominated deputy in the case of services under the supervision of the IT Office.

   (*b*) Any authorisation is subject to compliance with the College's statutes and regulations, including these regulations, and will be considered to be terminated by any breach or attempted breach of these regulations.

   (c) Authorisation will be specific to an individual.

8. Any password, authorisation code, etc. given to a user will be for his or her use only, and must be kept secure and not disclosed to or used by any other person. Exceptions may be made for accounts set up specifically to carry out business functions of the College.

9. Users are not permitted to use College IT or network facilities for any of the following:

   (*a*) any unlawful activity;

   (*b*) the creation, transmission, storage, downloading, or display of any offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the use of the facilities for properly supervised research purposes when that use is lawful and when the user has obtained prior written authority for the particular activity from the Governing Body.

   (*c*) the creation, transmission, or display of material which is designed or likely to harass another person in breach of the College's Code of Practice on Harassment;

   (*d*) the creation or transmission of defamatory material about any individual or organisation;

   (*e*) the sending of any e-mail that does not correctly identify the sender of that e-mail or attempts to disguise the identity of the computer from which it was sent;

   (*f*) the sending of any message appearing to originate from another person, or otherwise attempting to impersonate another person;

(*g*) the transmission, without proper authorisation, of e-mail to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of e-mail which is intended to encourage the propagation of copies of itself;

(*h*) the creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;

(*i*) private profit, except to the extent authorised under the user's conditions of employment or other agreement with the College; or commercial purposes (including advertising commercial services) without specific authorisation;

(*j*) gaining or attempting to gain unauthorised access to any facility or service within or outside the College, or making any attempt to disrupt or impair such a service;

(*k*) the deliberate or reckless undertaking of activities such as may result in any of the following:

- the waste of staff effort or network resources, including time on any system accessible via the College network;
- the corruption or disruption of other users' data;
- the unauthorised access, transmission or negligent loss of data;
- the violation of the privacy of other users;
- the disruption of the work of other users;
- the introduction or transmission of a virus or other malicious software into the network;

(*l*) activities not directly connected with employment, study, or research in the College (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation.

10. All College IT usage must conform to the College's *Prevent* duty policy.

11. Users shall treat as confidential any information which may become available to them through the use of such facilities and which is not clearly intended for unrestricted dissemination; such information shall not be copied, modified, disseminated, or used either in whole or in part without the permission of the person or body entitled to give it.

12. No user may use IT facilities to hold or process data relating to a living individual save in accordance with the provisions of current data protection legislation

(which in most cases will require the prior consent of the individual or individuals whose data are to be processed).

13. Any person wishing to use IT facilities for such processing is required to inform the College Data Protection Officer in advance and to comply with any guidance given concerning the manner in which the processing may be carried out.

14. Any person responsible for the administration of any College computer or network system, or otherwise having access to data on such a system, shall comply with the provisions of the University 'Statement of IT Security and Privacy Policy'.

15. Users shall at all times endeavour to comply with policies and guidance issued from time to time by College to assist with the management and efficient use of the College's ICT facilities.

16. Connection of any computer, whether college, departmental, or privately owned, to the College network is subject to the following additional conditions:

    (*a*) Computers connected to the College network may use only network identifiers which follow the University's naming convention, and are registered with the University IT Services. Please see users' guide for IT in St John's College for a description of the University allocation of email addresses.

    (*b*) The University's Trade Mark and Domain Name Policy specifies, *inter alia*, that all university activities (other than those within OUP's remit) should be presented within the ox.ac.uk domain. Any exception to this requires authorisation as defined in that University Policy.

17. Owners and administrators of computers connected to the College network are responsible for ensuring their security against unauthorised access, participation in 'denial of service' attacks, etc. In particular, they are responsible for ensuring that anti-virus software is installed and regularly updated, and that rules and guidelines on security and anti-virus policy, as issued from time to time by the IT Committee, are followed.

18. The College may temporarily bar access to any computer or sub-network that appears to pose a danger to the security or integrity of any system or network, either within or outside Oxford, or which, through a security breach, may bring disrepute to the College.

19. Providers of any service must take all reasonable steps to ensure that that service does not cause an excessive amount of traffic on the College's internal network or its external network links.

20. The College may bar access at any time to computers which appear to cause unreasonable consumption of network resources.

21. Hosting Web pages on computers connected to the College network is permitted subject to the knowledge and consent of Academic Services Committee.

22. It is not permitted to offer commercial services through Web pages supported through the College network, or to provide 'home-page' facilities for any commercial organisation, except with the permission of Governing Body, this permission may require the payment of a licence fee.

23. Use of file-sharing technology and participation in distributed file-sharing networks may be subject to additional regulation and restriction in order to prevent excessive use of College network resources, or the use of those resources for purposes unconnected with the College.

24. No computer connected to the College's network may be used to give any person who is not a member or employee of the University or its colleges access to any network services outside the College where that computer is situated.

25. Certain exceptions may be made, for example, official visitors to the College.

26. Areas of doubt should be discussed with the Academic Services Committee.

27. Providing external access to College's network resources for use as part of any shared activity or project is permitted only if authorised by the Academic Services Committee, and will be subject to any conditions that it may specify.

28. If any computer connected to the network or a sub-network does not comply with the requirements of this section, it may be disconnected immediately by the Network Administrator or any other member of staff duly authorised by the head of the college, section or department concerned.

29. If a user is thought to be in breach of any of the College's statutes or regulations, including these regulations, he or she shall be reported to the appropriate officer who may recommend to Governing Body that proceedings be instituted under College disciplinary procedures.

30. Access to facilities may be withdrawn.

Examining Users' Data

31. All staff of the IT facility who are given privileged access to information available through that facility must respect the privacy and security of any information, not clearly intended for unrestricted dissemination, that becomes known to them by any means, deliberate or accidental.

32. System Administrators (i.e. those responsible for the management, operation, or maintenance of computer systems) have the right to access users' files and examine network traffic, but only if necessary in pursuit of their role as System Administrators.

33. They must endeavour to avoid specifically examining the contents of users' files without proper authorisation.

34. If it is necessary for a System Administrator to inspect the contents of a user's files, the procedure set out in paragraphs (*2b*)-(*2e*) below must be followed.

35. Normally, the user's permission should be sought.

36. Should such access be necessary without seeking the user's permission, it should, wherever possible, be approved by an appropriate authority prior to inspection.

37. If it has not been possible to obtain prior permission, any access should be reported to the user or to an appropriate authority as soon as possible.

38. For the purposes of these regulations 'appropriate authority' is defined as Governing Body.

REGULATION HISTORY

Date of GB approval	***Brief summary of changes***	***Confirmation that linked documents have updated if necessary***	***College policy register updated***
June 2016	Generation of regulations	Confirmed	Yes (Sandra Campbell)
March 2017	Policy reviewed by Committee	Confirmed	Yes (Sandra Campbell)
	Wording changed: (Paragraph 4*a*) the College provides computer facilities and access to its computer networks only for purposes directly connected with the work of the University and the colleges and with the normal academic activities of their members. Wording replaced with the following to be in line with the University Policy: Users are not permitted to use College IT or network facilities for any of the following: activities not directly connected with	Confirmed	Yes (Sandra Campbell)

	employment, study, or research in the University or the colleges (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation. Paragraph 49, 54, 55 - IT committee has been changed to Academic Services Committee		
March 2018	Policy reviewed by Committee and subsequently approved by GB	Confirmed	Yes (Sandra Campbell)
Jan 2019	Minor numerical changes made. Policy reviewed by Committee and subsequently approved by GB	Confirmed	Yes (Sandra Campbell)
Feb 2020	Policy reviewed by Committee and subsequently approved by GB	Confirmed	Yes (Kate Doornik)
Jan 2021	Policy owner changed to Principal Bursar. Policy reviewed by Committee and subsequently approved by GB	Confirmed	Yes (Sandra Campbell)
Jan 2022	Updated University link. Policy reviewed by Committee and subsequently approved by GB	Confirmed	Yes (Iris Burke)