NEW COLLEGE
OXFORD

POLICY DOCUMENT

Email Confidentiality Code of Conduct for Staff

Overview

All employees working for the College are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within GDPR which came into force on May 25th 2018.

This means that employees are obliged to keep any personal identifiable information strictly confidential. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care (e.g. business "in confidence" information).

The College is committed to the delivery of the highest level of confidentiality for all the students and staff information must be processed fairly, lawfully and with as much transparency as possible so that the public and staff:

- Understand the reasons for processing personal information
- Give their consent for disclosure and use of their personal information
- Have complete trust in the way the College handles its information
- Understand their rights to access information held about them

The principle behind this Code of Conduct is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the College's security systems or controls in order to do so.

The University provided email system (Office365) has inherent risk associated with it regarding data security. As staff move from unit to unit during their career life within the University their email moves with them. The College sees this potentially as an extremely high-risk exercise, and a significant breach of confidentiality and data protection principles; where the information about one college is then kept in an e-mail account which is no longer associated with them and may be passed down to another college which is another altogether separate legal entity. Further, there is a breach of the GDPR in relation to data retention. Data retention schedules cannot be enforced if the data is no longer under the direct control of the college.

Email Usage Policy

Statement of authority and scope

This Policy is intended to detail the rules of conduct for all members (staff and students) of the College who use email and related services. This Email Policy applies to the use, for the purpose of sending or receiving email messages and attachments, of any IT facilities, including hardware, software and networks, provided by the College. The Policy is applicable to all members of the College including staff, students and other authorised users of College IT facilities.

Statement of responsibilities

Individual users are responsible for their own actions. The use of email facilities by individuals at the College assumes and implies compliance with this Policy, without exception, and with all those Acts, Policies and Regulations referenced below as enacted or authorised by the College or other regulatory bodies. Every user of email systems has a duty to ensure they practice appropriate and proper use, and must understand their responsibilities in this regard.

Senior management will be responsible for ensuring heads of Departments are aware of this Policy; they in turn will be responsible for informing their people of this policy.

Acceptable use

General

The College's main purpose in providing IT facilities for email is to support the teaching, learning, research, and approved business activities of the College. IT facilities provided by the College for email should not be abused. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- creation or transmission of material which brings the College into disrepute
- creation or transmission of material that is illegal
- the transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind
- the unauthorised transmission to a third-party of confidential material concerning the activities of the College
- the transmission of material such that this infringes the copyright of another person, including intellectual property rights
- activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users
- activities that corrupt or destroy other users' data or disrupt the work of other users
- unreasonable or excessive personal use (see 'personal use' below)
- creation or transmission of any offensive, obscene or indecent images, data or other material (other than for reasons specified in 'research and related' below)
- creation or transmission of material which is designed or likely to cause annoyance, inconvenience or anxiety
- creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs
- creation or transmission of defamatory material or material that includes claims of a deceptive nature
- activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals
- creation or transmission of anonymous messages or deliberately forging messages or email header information (ie without clear identification of the sender), or for 'flaming' - posting or sending offensive messages over the Internet.

- the deliberate unauthorised access to services and facilities accessible via JANET
- the unauthorised provision of access to College services and facilities by third-parties

Personal use

The College permits the use of its IT facilities for email by students, staff, and other authorised users for a reasonable level of personal use. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- a level of use that is not detrimental to the main purpose for which the facilities are provided
- priority must be given to use of resources for the main purpose for which they are provided
- not being of a commercial or profit-making 'business' nature
- not be of a nature that competes with the College in business
- not be connected with any use or application that conflicts with an employee's obligations to the College as their employer
- not be against the College's or University's rules, regulations, policies and procedures and in particular this Email Policy

All correspondence and activities for personal use are subject to review and investigation by the College. The College takes ownership of any data processed on its e-mail accounts and network and declares itself as the Data Controller for such data.

All information and data whether it is personal or not will be subject to the provisions of the Data Protection Act 2018 and the General Data Protection Regulation identifying the College as the Data Controller. This means that all information exchanged and/or processed for personal purposes may be disclosable. The College as the Controller of such data is committed to honour the rights of Data Subjects in both personal and professional correspondence.

Research and related

It is recognised that, in the course of their work or research, individuals of the College may have a requirement to transmit or receive material that would normally be defined as offensive, obscene, indecent or similar.

Incident handling and data protection

The College will investigate complaints received from both internal and external sources about any unacceptable use of email that involves Computing Services IT facilities. Computing Services, in conjunction with other departments as appropriate, will be responsible for the collation of information from a technical perspective. It should be noted that logs are only kept for limited periods of time so the prompt reporting of any incidents which require investigation is recommended.

Where there is evidence of an offence it will be investigated in accordance with the College/University's disciplinary procedures applicable to all members of the College. In such cases Computing Services will act immediately with the priority of preventing any possible continuation of the incident- hence email accounts may be closed or email may be blocked to prevent further damage or similar occurring.

Ending employment at the College

When at the end of your employment at the College, College will require that all email dealing with sensitive College information or containing personal data under GDPR protection that concerns the members of the College shall be deleted from your account and made irretrievable. No data shall be saved to external storage devices or forwarded outside the email system.

March 2019