Keble College IT Acceptable Use Policy (Students)

Keble College provides IT and network facilities subject to the terms and conditions stated in this policy. This policy in no way limits the applicability or obscures the intentions of any other policy or legislation that already governs IT and network use at Keble College or the University of Oxford.

Any activity that involves Keble College IT facilities must be carried out in accordance to this acceptable use policy. These rules must be read and understood before using any IT facilities at the college, and a signed declaration form must be returned to the College Office before use of any IT facilities is authorised.

1. **Definition of Terms**
   1. The term IT facilities shall be taken to include: free standing computers; networked computers; shared computers and terminals; services or software; networking that connects computers to any other computers or servers; computer peripherals; computer media; hardware components; networked resources; manuals and documentation.
2. **External Conditions of Use**
   1. Many IT facilities available at Keble College are provided through contractual agreements with third party organisations, most notably including the network connection to the University of Oxford and to the UK academic network (JANET). Users of these IT facilities must also abide by the terms and conditions of those agreements.
   2. Of particular importance is the JANET Acceptable Use Policy, provided by UKERNA (http://www.ja.net/documents). This must be read prior to using any IT facilities at Keble College.
   3. Other requirements specific to IT use currently include:
      a. University Regulations Relating to the use of IT Facilities
      b. Computer Misuse Act (1990)
      c. Data Protection Act (1998)
      d. Oxford University disclaimer of liability
      e. CHEST Code of conduct
      f. Microsoft Campus Agreement
      g. Terms and conditions for other licensed software
3. **Authorisation to use IT Facilities**
   1. Authorisation to use IT facilities may only be granted by the IT Manager, Bursar or Warden of Keble College.

2. It is not permitted for authorised users to allow use of IT facilities provided by Keble College by any other person.

4. Acceptable Use

1. Keble College IT facilities, including the use of the network from personally-owned equipment, may under no circumstances be used for conducting business or other commercial activities. The following actions are not considered to be covered by this clause:

   a. Application for jobs and sending of CVs via email;

   b. Conducting business transactions as a customer (purchasing items online);

2. Users of IT facilities provided by Keble College are not permitted to use those facilities for any of the following:

   a. Any unlawful activity;

   b. The creation, transmission, storage or display of any obscene, offensive, indecent or menacing images, data or other material or any data capable of being resolved into such images or material;

   c. The creation or transmission of any material designed or expected to harass another person, or to cause annoyance, inconvenience or needless anxiety;

   d. Access to, creation, transmission or display of extremist material which has the real potential to lead to serious terrorist crime on the part of the user or to draw others into terrorism (contrary to the College and University's statutory duty under *Prevent*);

   e. The sending of any email which does not correctly identify the sender, or which attempts to disguise either the sender or the computer from which it was sent;

   f. The creation or transmission of defamatory material about any individual or organisation;

   g. The creation or transmission of material that infringes a copyright, trade mark, moral right or other intellectual property right;

   h. The transmission of email to a large number of recipients without proper authorisation, unless those recipients have given consent to receive such email;

   i. The sending or forwarding of email intended to encourage the propagation of copies of itself;

   j. Commercial purposes or conducting business, except to the extent authorised under the user's agreement with the college;

   k. Attempting to gain unauthorised access to any IT facility, system or service within Keble College or outside, or making any attempt to disrupt such a service;

l.   Deliberate or reckless undertaking of any activities which may result in any of the following:

- Introduction or transmission of a virus into the network or any computer systems or servers;
- Corruption of data or disruption of the work of others;
- The waste of network or system resources on systems provided by or accessible through Keble's IT facilities;
- The waste of staff effort investigating and dealing with any deliberate infraction.

5. **Monitoring and Control**

   1. Keble College IT facilities are managed and maintained by appointed system administrators who are the IT Manager and IT Officer.
   2. The system administrators reserve the right to monitor the usage of IT facilities, including network traffic, either to investigate an alleged breach of this policy or to identify problems with the IT facilities and infrastructure.
   3. Any records taken or data captured will be retained only for a length of time appropriate to the investigation or fault and will be held securely.
   4. Any data captured will be restricted as far as possible to only examine the particular protocols and sessions needed to minimise the risk of capturing any personal data not relevant to the investigation or fault.

6. **Connection of Personal Equipment to the Network**

   1. Use of personal equipment connected to the Keble network shall be in accordance with the terms and conditions set out in this policy.
   2. The owner, administrator and users of any equipment connected to the Keble network shall be jointly responsible for taking all reasonable precautions to ensure that the equipment does not disrupt the network or other systems connected to it, or breach this policy. In particular, it is a requirement that:

      a.   All available security updates shall be installed in a timely fashion;

      b.   Where applicable, a suitable anti-virus product shall at all times be installed, operational and constantly kept up-to-date so as to provide an effective prevention against viruses and malware.

      c.   Network accessible services should be disabled or appropriately restricted if they are not critical to the functioning of the equipment on the network or for the purposes it is intended.

      d.   In the event that personal equipment connected to the Keble network is detected to be in breach of regulations or an official report of misuse is received, it is a requirement that Keble IT staff be permitted to inspect the equipment to ensure that the reasons for the breach are dealt with correctly and to allow Keble IT staff to certify to any external organisation that action has been taken.

3. Equipment connected to the network must only use network identifiers allocated by Keble College. These identifiers and the unique identifier belonging to the equipment must not be modified to impersonate another device.
4. Equipment connected to the college network must not be used to provide access to IT facilities belonging to either Keble College or to the University of Oxford to persons not otherwise authorised to use those facilities.

7. **Reporting of Problems**
    1. Problems and general enquiries may be directed to the IT Department either by email to it-support@keble.ox.ac.uk or by telephone to 01865 (2)72788.
    2. If reporting a problem outside office hours then messages may be left at the Porters' Lodge.
    3. Any problems or faults with IT facilities should be reported in a timely manner so that the IT Department can make arrangements.