Directorate of Finance and IT

Guidelines for the Electronic Transmission of Data to Third Parties
Version 1 January 2009

1. Introduction

These guidelines are designed for all staff to observe. All members of the University have access to potentially confidential and personal data, and these guidelines are designed to minimise the risk of unauthorised disclosure of this information.

IT security has been increasingly being publicised in the national press and information security is of a high concern to the University.

All staff are responsible for the security of any data and in the event that any such information is transmitted from the University will be expected to take all necessary steps to ensure its continued security. Guidelines for the transmission of data are set out in this document and staff are expected to observe these as a basis for ensuring security of data for which they are responsible. In the event that security is breached, these guidelines would be evidential in terms of any decision to take further action including disciplinary action.

2. Personal and Confidential Data

Confidential data is defined as information about the University, its activities, the activities of its partners, staff or students, which is not for public consumption and should only be considered by authorised persons. Personal data is defined as data that is held and processed by the University that is related to living individuals that can be identified by this data. Both of these types of data are considered to be ‘sensitive’ data.

3. Verification of Recipient of Data

Any data, described as sensitive (as above) should **never** be released to any unauthorised individuals. It is the responsibility of the person transmitting the data, (in hard copy or by electronic means such as email) to ensure that the person receiving the data is authorised to do so. This is particularly important when dealing with email requests for data.

Any request for data should not be taken on face value. University employees are expected to check the identity of the recipient of the data by multiple means, i.e. telephone and email correspondence.

If you are at all unsure about the release of any data, do not release it. Speak with your line manager in the first instance, or contact the Secretariat for advice on the release of data under the Data Protection Act.

Information on the Data Protection Act can be found on the Planning and Secretariat web-pages:
http://www.keele.ac.uk/admin/ps/governance/Data_protection/dpa_home.htm

4. Using Email to Transmit Data

Email communications, although fast, effective and easy to use, are NOT a secure method of communication. The University recognises that there is some data that must be transmitted to authorised recipients using email, however, email is not a preferred transmission of data tool and if possible, efforts should be made to encrypt any data sent in this format.

Members of staff are advised to consider, when using email, whether data that is being transmitted could be considered as personal or confidential, and if so, can this data be transmitted in any other format.

4.1 Emailing University Colleagues.

Sending emails to colleagues, using their Keele email address is considered secure. You should always ensure that emails containing confidential or sensitive data are sent to the correct recipient(s) though.

4.2 Using Mark-Up

Unless there is good reason to do so, it is strongly recommended that the mark-up utility is NOT used within Word documents transmitted via email. This is because the mark-up can be "undone" and there may be inappropriate text in earlier versions of the document.

5. Using Alternative Transmission Processes

The University wishes to encourage the use of encryption when transmitting personal or confidential data. Encryption can be achieved by sending by post, documents stored on a password protected memory stick. It is recommended that this is sent via recorded delivery.

Staff using this method should contact the IT Services Help Desk to obtain details of recommended memory sticks. It should be possible to ask the recipient to return them. The recipient would have to be informed of the PIN number of the memory stick, so staff should ensure they inform the recipient by phone. The Passwords/PIN should **never** be transmitted with the memory stick.

6. Identified Individuals working with Sensitive Data

The University has identified a number of individuals who are expected, as part of their daily working activities, to work with a high level of personal and confidential data.

Those individuals will receive tailored training on the use of encryption and suggestions for the safest ways to work with their data. For further details on this, please contact the Data Protection Officer in Planning and Secretariat.