2.6 Privacy and Monitoring Policy

“The University requires that staff, students and others making use of the University’s ICT-based systems are aware that activity logging takes place, and that monitoring or content inspections of an individual’s activity may occur under specific circumstances.”

The policy describes the specific circumstances where the University may need (or be required) to examine the usage logs and datasets of users of University IT systems. This policy describes both the circumstances and the process that will be followed.

http://url.tees.ac.uk/pmp

2.7 IT Administrative Privileges Code of Conduct

“The code of conduct defines how administrator privileges on University owned workstations and laptops are to be used. The document also defines how users with standard rights may apply for this access, and what they may use this access for.”

http://url.tees.ac.uk/apcc

2.8 Guidance for the use of Social Media

“Social media tools such as blogs, online forums, content-sharing websites and other digital channels established for online interaction and connection are increasingly used to: Promote Teesside University to colleagues, students, customers, the media and other stakeholders; Share personal opinions and participate in online dialogue; Support learning and teaching.”

The guidance covers both intended and unintended outcomes of the use of Social Media which staff, in particular, should be aware of. Clarity around the source of opinion in terms of it being personal or representative of the University is important.

http://url.tees.ac.uk/gsm

3. BREACH OF POLICY

Please be aware that the above policies have varying clauses to cover breach of policy. Breach of policy may result in disciplinary action being taken.

Paul Lambert, IT Director.

Further copies of this leaflet may be obtained from: http://url.tees.ac.uk/pol

Teesside University

IT POLICY OVERVIEW

Staff/Student Guidance

This document provides an overview of IT related policies with which staff, students and other authorised users of University IT facilities need to comply.

1. OVERVIEW

This document provides an overview of IT related policies with which staff, students and other authorised users of University IT facilities must comply.

2. THE POLICIES

Below is a list of IT related policies together with the key policy statement and some brief additional information. This information is designed to guide the reader in understanding the nature of policies; it is not a replacement for reading the policies themselves.

2.1 Information Security Policy

“The purpose of this Policy is to safeguard information belonging to the University and its stakeholders (third parties, clients or customers and the general public).”

This is a high level policy that describes how information and information systems are to be managed. Many of the other policies listed below are subsidiary to this one.

http://url.tees.ac.uk/isp

2.2 IT Acceptable Use Policy

“This policy applies to anyone using Teesside University IT facilities (hardware, software, data, network access, third party services, online services or IT credentials) provided or arranged by Teesside University.”

All users of any University IT facilities must be familiar with the IT Acceptable Use policy. It comprises a short policy section with extensive guidance on use. The primary focus is to ensure the reader is aware of what is and is not permissible when using University IT facilities.

http://url.tees.ac.uk/aup

2.3 IT Hardware Asset Management Policy

“The University requires that all IT hardware, particularly data bearing portable equipment, is properly managed throughout its lifetime.”

This policy is primarily concerned with tracking IT hardware assets from the perspective of avoiding data loss. It mostly affects staff and the policy describes the separate responsibilities of Schools / Departments, individuals and the IT Department.

http://url.tees.ac.uk/ham

2.4 IT Software Asset Management Policy

“The University requires that all software installed on University equipment is properly licensed.”

This policy informs everyone of the requirements with regard to purchasing, loading and using software on University equipment.

http://url.tees.ac.uk/sam

2.5 Remote Working Policy

“This policy is concerned with the technical and security aspects of facilitating remote, generally off campus, access to University information systems for University staff.”

The policy covers the use of both data transports (protocols permitting live remote access to University information and systems) and data transfers (the use of storage devices to transport data for remote working).

http://url.tees.ac.uk/rwp