Teesside University

IT Administrative Privileges Code of Conduct

1. Purpose

The purpose of this document is to define how local administrator privileges on University owned workstations and laptops are to be used. This document also defines how users with standard rights may apply for this access, and what they may use this access for.

By default, staff are provided with standard privileges on their desktop/laptop as well as full Service Desk support, data backup (via U:\ drive and shared drives) and anti-virus protection.

However, exemptions **may** be granted by IT Services senior management (delegated through the Information Assurance Team only) to staff members who require administrator privileges to perform job related tasks. Such staff are **bound to the terms stipulated below,** failure to observe them could constitute a breach of University policy. Students are not entitled to administrator privileges on University maintained computers.

When considering applying for administrative privileges for your computer, you should appreciate that running a computer system with administrator privileges may represent a significant risk to the confidentiality, integrity and availability of the University's information assets.

It is also unnecessary for the majority of staff. These privileges **must** be agreed by a senior member of staff of the requesters dept./school.

2. The Code of Conduct

This document is an adjunct to the University’s Acceptable Use Policy (specifically section 6.6).

The University requires all users to exercise a duty of care in relation to the operation and use of its computer and information systems.

2.1 Why you may need administrative privileges (standard users)

- Installation of software. To evaluate or install software that is vital to your role at the University. The preferred route for this operation is **always** via the IT Service desk. Any software installed **must** comply with the University Software Asset management policy

- System Settings: changing system settings such as the date\time or network configuration settings require administrator privileges. (this may be necessary on a laptop whilst visiting a different country)
- Legacy or Poorly Coded Software: some applications simply require administrator rights to run normally.

2.2 Why you may need administrative privileges (IT Services staff)

- To perform necessary support operations.

2.3 The Use of Administrator Privileges (standard users, Windows platform)

Once granted, you will be supplied with a special account, which will take the form of “UxxxxxxxPC”. This account will have administrative privileges on the PC that you specify in your request. You may use this account to

- Install software
- Configure low-level hardware, e.g. personal printers, scanners at home with a laptop
- Run legacy software

This can be done by running setup(s) etc. by right clicking on an object and selecting “Run As” or “Run As Administrator” This is the only acceptable use of the PC account

You agree that you will not:

- Login with this account, or use this account as an alternative to your standard user account.
- Alter the security settings of the device to enable wider access to administrator privileges. E.g. No changes to Local Administrator Groups

  Any such changes would be a contravention of the University’s IT Acceptable use policy (section 6.6)

  “Teesside University has taken measures to safeguard the security of its IT infrastructure, including things such as antivirus software, firewalls, spam filters, security permissions and so on. You must not attempt to subvert or circumvent these measures in any way.”

  Breaching this policy could lead to formal disciplinary processes.

  (For other Operating systems, contact ITaCS for guidance)

2.4 The Use of Administrator Privileges (IT Services staff, Windows platform)

ITaCS support staff require access to administrator privileges on the entire PC estate to perform their necessary tasks. Accounts with administrative privileges may cause considerable damage in the wrong hands, so a Multi-Factor Authentication (MFA) method is used to control usage.

IT Services Information Assurance team will provide a MFA device (currently a YubiKey) to enable administrator privileges to IT Services staff – to perform necessary administrative support operations.

Administrative privileges can be gained by running setup(s) etc. by right clicking on an object and selecting "Run As" or "Run As Administrator" and using the Yubikey device to authenticate This is the only acceptable use of the YubiKEY device. Please note:

- Administrative privileges gained by YubiKEY **must not** be used to alter the security settings of the device to enable wider access to administrator privileges. E.g. No changes to Local Administrator Groups

  Any such changes would be a contravention of the University's IT Acceptable use policy (section 6.6)

  "Teesside University has taken measures to safeguard the security of its IT infrastructure, including things such as antivirus software, firewalls, spam filters, security permissions and so on. You must not attempt to subvert or circumvent these measures in any way."

  You are also reminded of section 4.2 of the Acceptable use policy, in that your use of admin privileges *"should be in a manner that is consistent with your role."*

  (For other Operating systems, contact IT Services for guidance)

2.5 Breach

IT Services staff may, at any time, perform compliance checking of issued administrator privilege accounts and any deviation from the conditions laid out in this code of conduct will result in the removal of the administrative privileges.

Individuals in breach of the IT Acceptable Use Policy are subject to disciplinary procedures at the instigation of the relevant Dean/Director

3. Ownership

3.1 The Director, IT and Communications Services has direct responsibility for maintaining this code of conduct and providing guidance and advice on its implementation.