Policy on the Acceptable Use of IT Facilities (AUP)

(Standard Version)
Please read the statement and sign.

Staff

College staff undertake to comply with the provisions of this AUP, either by signing an electronic version of this AUP (as part of the registration process); or by physical signature on a copy of this AUP.

Staff employed via the College Supply Pool or through external agents to follow the process for 'Third Parties'.

Students

A student confirms acceptance of this AUP by enrolling with the College. Once a student enrolment is confirmed by CIS, user privileges are conferred and compliance with this AUP will be required for as long as user privileges are extended. Students are informed of their obligations when they are supplied with their network account.

Third Parties

In order to register a third party user of IT facilities, a College Manager should a complete a Staff Network Registration Form on the Intranet, which is forwarded automatically to ICT. Before user privileges can be conferred a completed copy of this AUP must be signed by the third party user and forwarded to ICT Services (G.1.16).

Please read through this policy carefully; by signing this document or accepting a contract of employment with the College you are asserting that you have read and understood this policy. If you do not comply with its provisions you may have your network privileges withdrawn and may be subjected to disciplinary or legal action.

Policy

A registered user may use the College network and computer equipment for any legal activity that is in furtherance of the aims and policies of the College. In registering, a user accepts the terms of the College's Policy on Management and Monitoring of Electronic Communications, Internet and Telephones and the Data Protection Policy and undertakes to comply with the statements below.

User Login and Password

All users who require access to the College Network are required to have a legitimate user login and password. Users must adhere to the following:
- Do not attempt to gain unauthorised access to College IT systems;
- Passwords must never be written down or disclosed to another individual or organisation;

- When a new password is issued (either for a new account or a properly validated password reset) the user must logon at the first available opportunity, at which stage the system will prompt the user to change their password.

You must not use the College IT facilities for any of the following:
- deliberately attempting to gain access to restricted areas within the College or other locations;
- visiting, viewing, transmitting or downloading any Internet material which is counter either to legislation, College policies (eg equal opportunities, bullying and harassment) or to commonly accepted standards, or is likely to be offensive or indecent to reasonable people. This includes inappropriate websites including those promoting extreme Islamic or right-wing ideologies as well as material concerning the purchase of firearms. Members of staff may access this kind of material only for bona fide academic purposes;
- the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- the download, copying or transmission to third parties the works of others without their permission. Written material, images and software are protected by the laws on copyright;
- the transmission of unsolicited commercial material;
- corrupting or destroying other users data;
- violating the privacy or disrupting the work of others;
- using the network in a way that denies service to other users, for example, deliberate or reckless overloading of the network or computers;
- deliberately introducing viruses onto the College network;
- place on the Internet any material, which incites, encourages or enables others to gain unauthorised access to the College's computer system.

In addition, unless agreed with the Head of ICT, a user <u>must not</u>:
- install hardware on an individual PC;
- attach devices to an individual PC or VDI;
- subscribe to Internet services via the College network;
- load, install or modify software;
- encrypt data (the College will remove any encrypted data from the systems).

Specifically, a third party user with no contract of employment <u>must not</u>:
- access or copy personal or confidential data without the **explicit authorisation** of the College. If access to such data is required, a data sharing agreement must be completed. In this instance please contact the Information and Records Team on records@newdur.ac.uk

To be signed in all cases (A typed name in place of a signature is **not** acceptable):

I have read and understood this Acceptable Use Policy and agree to comply with its provisions.

Signed _____

Name *(Please Print)*_____ Date _____

Staff AUP (V10)/Accessibility Checked/June 2019