New College Durham

Electronic Communications Policy

Procedure Title	**Electronic Communications Policy**
Document Owners	**Academic Registrar/DPO** **Executive Director of ICT and Corporate Services** **Executive Director of Human Resources and Corporate Services**

Directorates and Departments affected by this Procedure	**All staff and students**
Procedure Effective From	**April 2025**
Next Review Date	**April 2027**

We will consider any request for this procedure to be made available in an alternative format.

We review our policies and procedures regularly to update them and to ensure that they are accessible and fair to all. All policies and procedures are subject to impact assessments. Equality Impact Assessments and Accessibility Checks are carried out to see whether the policy has, or is likely to have, a different impact on grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation or human rights.

We are always keen to hear from anyone who wants to contribute to these impact assessments and we welcome suggestions for improving the accessibility or fairness of the policy.

To make suggestions or to seek further information please contact records@newdur.ac.uk

Equality Impact Assessed: January 2025

Accessibility Checked: March 2025

Contents

1. Introduction

This policy describes responsibilities and requirements for the management and monitoring of electronic communications to maintain compliance with legal obligations and other College policies.

This policy also contains guidance on expected use of these facilities by staff and students as well as information on how the College intends to monitor this use.

2. Scope

This policy applies to anyone who accesses the College network, including users of College-owned devices and non-College-owned devices. This encompasses both on-site and off-site access to College facilities, electronic communications, and internet services.

3. Responsibilities

The Senior Information Risk Owner requires this policy to be in place and will provide senior management support.

The Academic Registrar has responsibility for ensuring this policy is in place and is reviewed as necessary by the Executive Director of ICT and Corporate Services and the Executive Director of Human Resources and Corporate Services. There is a joint responsibility for ensuring guidance is available and promoting compliance with the policy.

All staff are responsible for familiarising themselves with this policy as directed in their contract of employment.

Compliance with this policy is compulsory for all users of College equipment and IT services. Anyone who fails to comply with the policy may be subjected to action under the College's disciplinary policies. It is the responsibility of Heads of Department/Schools and their Directors/Assistant Principals/Vice Principals/Deputy Principals to ensure that staff and students are aware of the existence and content of the policy.

4. Relationship with existing policies and legislation

This policy has been formulated within the context of the following College policies.

- Staff Code of Conduct
- Data Protection Policy
- All Safeguarding Policies
- PREVENT Duty for Staff Policy and Procedure

- Records Management Policy
- Acceptable Use Policy
- Information Security Policy
- Copyright and Intellectual Property Policy
- Social Media Policy
- M365 Management Policy
- AI Policy

This policy will facilitate compliance with the following legislation:

- Regulation of Investigatory Powers Act 2000
- Malicious Communications Act 1988
- General Data Protection Regulation
- Data Protection Act 2018 (incl. UK GDPR)
- Human Rights Act 1998
- Defamation Act 2013
- Copyright, Designs and Patents Act 1988
- Privacy and Electronic Communications Regulations 2003
- Counter Terrorism and Security Act 2015

5. Personal use of College facilities

The College telephone, electronic communications and Internet systems, including applications and devices supplied to enable their use, are provided for work and study related activities. Reasonable and appropriate personal use is permitted if users adhere to the College's **Acceptable Use Policy** and **Social Media Policy** and discard personal correspondence when no longer required. The College reserves the right to monitor telephone, electronic communications, device and Internet usage logs and, in specified circumstances, the content of any communications. Please refer to the section entitled 'Monitoring' for further information.

Any user who has been allocated a network account and/or a College device is responsible for all activities conducted using that account or device. Users must not use their College account to create a social media profile.

6. The Internet

Staff must also ensure they adhere to the College's **PREVENT Duty for Staff Policy and Procedure** and should especially try to be vigilant in reporting unauthorised or inappropriate use of the Internet by students, understanding that it is their duty to report incidents or concerns to the appropriate department. In most cases this would be the Head of ICT, however in relation to concerns about extremism or radicalism these should be reported to the College's PREVENT Co-ordinator / any of the Designated Safeguarding Leads.

There are sites to which the College will prohibit access using filtering software. The College is cognisant of the role web-filtering plays within its approach to online safety whilst avoiding over blocking that could negatively impact teaching and learning. The College has introduced a differentiated set of web filters for FE and HE students that recognise this demand. Where there is an educational requirement to allow access to a web location that is still blocked for research purposes or if you want to request that a certain site be prohibited under the College's **Acceptable Use Policy**, a staff member can make this request through an online process. They will need to provide an academic/ educational rationale and details of how they will safeguard the access to this site.

Attempts to access blocked/inappropriate sites may lead to action under College policies mentioned in section 4 above.

Unauthorised use of electronic communications and/or the Internet may expose both you personally and/or the College to Court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against the College for any legal action to which the College is, or might be, exposed as a result of your unauthorised use of the Internet.

7. Telephones

The College recognises that staff may occasionally need to make personal telephone calls. This use should be reasonable, and the College will monitor overall usage. Staff will be informed if their usage is seen as excessive or inappropriate. Any calls to premium telephone lines or any international personal calls will be chargeable to the member of staff unless cleared in advance by a line manager as necessary for College purposes. Some of these calls are already routinely blocked by the College and the rationale for this is determined by the Senior Postholders and managed by the Head of ICT.

It is not a requirement of the College that staff should have access to their College supplied mobile devices outside their normal working hours. However it is expected that staff provided with mobile devices for business purposes should be easily contactable via these devices during working hours.

Please note that where a member of staff is outside of the UK on personal travel, any College owned mobile phone should either be left secured in the UK or the data roaming feature should be switched off. Any member of staff wishing to make use of data roaming whilst outside the UK should obtain the budgetary consent from the Head of School/Department prior to travel.

8. Electronic communications

The College recognises the importance of electronic communications and encourages staff and students to use them in the performance of their duties and to

aid their study at the College. In the light of this all users should be aware that correspondence sent using College facilities and via College systems remains the property of the College and is liable to be disclosed in response to Freedom of Information and Data Protection requests.

College approved tools for texts, messaging and emails are MS Teams and Outlook. Other text and messaging apps must not be used to conduct College business and specifically must not be used to contact students unless expressly authorised by the SIRO, or nominated delegate, in writing.

Inappropriate use of electronic communications by a user may result in action under College formal procedures.

Note that where an email account or data storage allocation has been supplied by the College, the College will be able to access the data held in the manner described and for the purposes outlined in section 12 'Monitoring'.

9. Acceptable Conduct for Electronic Communications

- You are expected to **use MS Outlook and Teams as a means of communication** in your everyday work.
- You are expected to **check and respond** to business messages on receipt.
- You are expected to **maintain accurate records** of College business activities for as long as these are required by the College.
- You must **not keep personal data** any longer than necessary.
- You are expected to **ensure that information is protected** against the consequences of breaches of confidentiality and failures of integrity.
- You are expected to **provide advice and assistance** to persons making requests for information.
- You must **ensure electronic communications are managed** – that means actioned, filed or deleted as appropriate. These systems are for communication not storage/record keeping.
- **Do not speculate or make subjective or unsupported claims** about staff, students or any other person.
- Ensure **devices are not left unattended and unlocked** as you will be held responsible for all activity using your account.
- Contact the ICT Helpdesk **if you receive unsolicited and suspicious emails** that may represent a security threat

10. Meetings

Meetings must not be recorded unless all parties are aware and have consented. In these cases the purpose of the recording must be clearly communicated. In general it is not expected that meetings will be recorded.

Recording is expressly prohibited for sensitive discussions. This is specified within the relevant HR policies. Similarly, AI bots should not be admitted into meetings unless their function, such as transcription or note-taking, has been approved and disclosed to all participants, ensuring compliance with data protection and college policies. Unauthorised recordings or the undisclosed use of AI tools in meetings are strictly prohibited and may result in formal action if not adhered to.

11. Disclaimer

A disclaimer is included on all e-mails sent externally by staff. The text of the disclaimer will be subject to change to reflect prevailing circumstances.

12. Defamation and reputation

Electronic communications and the Internet are a form of publication, and their wrongful use may constitute a libel contrary to the provisions of the Defamation Act 2013. Staff and students must not put any defamatory statement onto the Internet using their College account or onto any of the College's computer systems.

Staff and students must not send messages or post information on the Internet (this includes Social Media sites) that could bring the College into disrepute.

13. Discrimination, bullying and harassment

The College does not tolerate discrimination, bullying or harassment in any form. This principle extends to any information distributed via College systems including electronic communications, the Internet or telephone. Neither staff nor students should put on any system any material that bullies, discriminates or encourages discrimination, bullying or harassment.

14. Monitoring

The College reserves the right, without notice, to access, listen to or read any communication made or received by staff or students on its computers or telephone system for the following purposes:

- to establish the existence of facts
- to ascertain compliance with regulatory or self-regulatory practices and procedures
- to investigate or detect unauthorised use of systems
- to prevent or detect crime
- to provide practical help to prevent people from being drawn into terrorism and violent extremism

- to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding e mails to correct destinations
- to check electronic communications systems when you are on holiday or on sick leave.

All monitoring must be undertaken by personnel who will be subject to security and confidentiality requirements and will be trained in Data Protection.

Teams chat and email is retained for 2 years.

Staff

Managers should not monitor their staff's e-mail, telephone or internet usage. Where an issue arises where there may be a case to monitor such usage, the manager will explain the concerns to the SIRO or nominated delegate and they will determine if monitoring is recommended.

In cases where targeted monitoring is recommended, the SIRO will make the decision to monitor a member of staff's email, telephone or internet usage before monitoring is actioned.

If information in relation to Trade Union activities is accessed, the relevant Trade Union Officer should be informed.

The College reserves the right to monitor time spent by staff accessing the Internet for browsing. The College will conduct monitoring of sites visited, the content viewed and/or information downloaded.

The College reserves the right to make and keep copies of telephone calls, electronic communications and data documenting use of the telephone, electronic communications and/or the Internet systems, for the purposes set out above.

Fob access to secure areas of the College will not be monitored and this data is only retained for 30 days and then deleted.

Students

Where an issue arises where there may be a case to monitor a specific student's usage of email or the internet, the Head of School will explain the concerns to the Head of ICT and they will determine jointly if monitoring is recommended.

The College reserves the right to monitor the activity of students accessing the Internet for browsing. The College will conduct monitoring of sites visited, the content viewed or information downloaded. This will be done to ensure adherence with the Acceptable Use Policy and the PREVENT Duty for Staff Policy and Procedure.

The College also reserves the right to make and keep copies of electronic communications and data documenting use of electronic communications and the Internet systems, for the purposes set out above.

15. Reporting misuse

Anyone who suspects misuse of the College electronic communications, Internet or telephone systems should in the first instance advise the Executive Director of ICT and Corporate Services and the Executive Director of Human Resources and Corporate Services.

16. Evaluation and review

The performance of this Policy will be reported on annually in the Information Governance Policies Annual Report to the Corporation and it will be formally reviewed every two years.

In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.