EMAIL AND INTERNET POLICY

1 Aims and Objectives

1.1 The College recognises that the Internet and email systems play a key role in the conduct of the College's business and that these systems support employees in carrying out their work efficiently. Nevertheless, the provision of Internet and email systems to employees does expose the College to a number of risks and liabilities. This Policy highlights those potential liabilities to ensure that employees understand how they should be avoided.

1.2 The College invests substantially in email and Internet systems and the facilities provided represent a considerable commitment of resources. This Policy informs employees of the College's expectations for the use of those resources to ensure that they are used appropriately.

2 Legislation

2.1 The College will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which is predominantly the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Data Protection Act 1998, the Human Rights Act 1998, the Counter Terrorism and Security Act 2015 and the Prevent Duty 2015.

3 Monitoring

3.1 Computers and email accounts are the property of the College and are designed to assist in the performance of employees' work. Employees should therefore have no expectation of privacy in any email sent or received or in the Internet sites that employees access.

3.2 The College will monitor email and internet use where it has a reasonable cause to do so. Staff members will be informed before monitoring takes place with the exception of monitoring under the Prevent Duty (2015). Proactive monitoring will take place to detect any material promoting terrorism, violent extremism or which may be used to radicalise our staff and student body (as defined by the Counter Terrorism and Security Act 2015 and the Prevent Duty 2015).

3.3 The College may exercise its right to intercept email and Internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons:

- To establish the existence of facts relevant to the College's business;
- To ascertain compliance with regulatory practices or procedures relevant to the College;
- To ensure that employees using the system are achieving the standards required;
- To prevent or detect crime;
- To investigate or detect the unauthorised use of Internet and email systems;
- To ensure the effective operation of the system, e.g. to detect computer viruses and to maintain an adequate level of security.
- To prevent or detect radicalisation and extremism.

3.4 Although an email that is clearly marked as private cannot be defined as a communication relevant to the College's business, the College reserves the right to monitor the content of such an email where there is a

reasonable belief that it may breach this Policy, for example by containing discriminatory or pornographic material.

3.5 For business continuity purposes, the College may need to check the emails of employees who are absent. The College will attempt to gain the permission of the employee concerned before monitoring emails in such circumstances.

3.6 To be able to exercise its rights (as described in clause 3.3, above), the College must have made all reasonable efforts to inform every person who may use the email and Internet systems that monitoring may take place. The College believes that the communication of this Policy to all employees meets this requirement. All emails will include a disclaimer at the end, which will advise external recipients and senders of email of the College's Policy (see clause 10, below).

3.7 The College reserves the right to use the content of any employee email in any disciplinary process:

3.8 Where the email accounts of union stewards or branch officers and reps need to be examined, stewards/branch officers will be consulted prior to examination and either the union steward/branch officer or a nominated representative will be present whilst such an examination takes place. This is to protect the confidentiality of emails from members.

3.9 Employees should note that all emails can be recovered even after they have been deleted.

3.10 The College reserves the right to inspect any files stored by employees in all storage systems in order to assure compliance with this Policy. This includes team and home folders.

3.11 The college will proactively monitor and address any attempt to access internet material which may promote terrorism, radicalisation or violent behaviour.

4 General Operating Principles and Personal Usage

4.1 The email and Internet systems are primarily for business use.

4.2 The College operates within a framework of mutual trust and recognises that in certain circumstances, particularly when there is a need to communicate urgently, it may be appropriate for employees to send and receive personal emails. **However, such reasonable private usage of email must not interfere with employees' work.** Excessive private use of the email system during working hours will lead to disciplinary action and may in certain circumstances be treated as gross misconduct. Employees must not use the College's email address as their main contact when registering for services and goods on-line. Hotmail, Yahoo and Gmail accounts can be set up by the employee for this purpose.

4.3 The College also recognises that there may be need for individuals to have to carry out personal tasks on the Internet whilst at work. However, where such a need arises, employees are required to limit their access to the Internet for personal usage to authorised breaks such as lunch breaks or just before or just after their normal working hours.
Personal use of the Internet during working hours may lead to disciplinary action and excessive personal use may in certain circumstances be treated as gross misconduct.

4.4 Personal usage of the email and Internet facilities must still adhere to the standards outlined in this Policy and in other College policies, such as the Bullying and Harassment Policy. Breaches of College policies through personal use of email and Internet will be dealt with under the College Disciplinary procedures.

4.5 The standards set out in this Policy are designed to minimise the risk of incurring liability in relation to employees' usage of email and Internet. For example, the College could be prosecuted under child protection

legislation if employees are found to have downloaded child pornography using College systems. The College will take disciplinary action against any employee who breaches any of the requirements contained in this Policy, which will include summary dismissal for those committing acts of gross misconduct.

4.6 The College's Grievance Procedure will be used to handle any disputes concerning the operation or application of this Policy.

4.7 Each employee is issued with a unique password for use of the College computer systems for security purposes. Employees are responsible for safeguarding their password. For reasons of security, employees must not print, store online or share their individual passwords with others. User password rights are given to employees for security purposes and should therefore not give rise to an expectation of privacy. A member of staff must not use their personal network account to log a PC on for a learner as this could give rise to a breach in the data protection act or security of the information.

4.8 You must not leave your PC logged on and unattended without ensuring that it is locked. (Press ctrl, alt, delete and then select lock).

4.9 All records, documents and other papers (or extracts thereof) made or acquired by staff in the course of their employment shall be the property of the Corporation. Staff who wish to copy documents in their home folders for themselves upon termination of employment should seek permission from their line manager before doing so.

5 Standard College Email Practice

5.1 Emails should be drafted with care. Due to the informal nature of email, it can be easy to forget that it is a permanent form of written communication and that material can be recovered even when it has been deleted. Employees should ensure that the content and tone of emails reflect the professional image of the College.

5.2 All emails should be composed without using 'text speak', this is deemed inappropriate. The standard college email signature should be attached to all emails. Guidelines and a template for signatures can be found on staff Moodle and Staffnet (under "Marketing – Logos, Templates and Resources").

5.3 Emails should be clear and concise and should not be any longer than necessary.

5.4 Employees should not send unnecessary emails, or copy other recipients into messages without good reason. Unnecessary emails waste recipients' time and congest the email system.

5.5 Employees should not attach unnecessary files as large attachments can congest recipients' systems. The maximum file size that can be attached on the College system is 10Mb; this is the maximum allowed by many Internet Service Providers. Should it be necessary to send or receive larger files this service is available and can be accessed by contacting the IT Helpdesk.

5.6 Emails should not be written in capital letters as this can be construed as shouting via email.

5.7 Hard copies should always be made of emails which need to be retained for record-keeping purposes.

6 Use of Email

6.1 Employees must never access another employee's email account; except in circumstances where an employee is absent from work and has given his or her express consent for a colleague to check his or her emails. Even where access is granted in such circumstances, employees must never send an email from that account;

instead response emails should be sent from the individual's own College email account, clearly marked as being "on behalf of" the original recipient.

This is separate to accessing a mailbox where you are a delegate on that account as you have already been given permission to access the mailbox.

6.2 Emails must not contain any message or image that is discriminatory (on the grounds of sex, race, disability, sexual orientation, gender identity, religion, belief or age), illegal, obscene, pornographic, abusive or threatening, or which promotes terrorism or violent extremism. The College does not tolerate discrimination, harassment or bullying and any breach of this rule will constitute gross misconduct.

6.3 Employees should not make derogatory remarks in emails about colleagues, students, competitors, employers or any other person. Written derogatory remarks could be considered to be defamation, which could give rise to legal action being taken against the author and/or the College.

6.4 Employees must not send confidential documents or disclose confidential College information by email. Secure forms of data transmission are available. Please contact the IT Helpdesk for details.

6.5 Employees must not enter into contractual commitments by email unless they have the necessary authorisation. It is easy for email to be viewed as an informal means of communication, but commitments entered into in emails will have the same weight and status as any other written contracts.

6.6 Employees must not begin or distribute chain emails or any other junk emails, including advertisements.

6.7 Employees must not send personal data of other employees, students, or clients via email, without the authorisation of the owners of that data.

Remember that when sending an email to multiple learners to use the BCC function rather than the 'To' function to avoid distributing a person's email address.

6.8 By sending emails on the College's system, employees are consenting to the processing of any of their personal data contained in that email and are explicitly consenting to the processing of any of their sensitive personal data contained in that email. If employees do not wish the College to process such data, they should communicate that information by other means.

7 Use of Internet

7.1 The College has software and systems in place that monitor and record all Internet usage. Therefore employees should not have any expectation of privacy in terms of their Internet usage.

7.2 Employees must not display, download, distribute, store, edit or record any material, including images, that are offensive, capable of constituting any form of discrimination (on the grounds of sex, race, disability, sexual orientation, gender identity, religion, belief or age), obscene, pornographic or paedophiliac. Any such action will be considered as gross misconduct.

If you accidentally arrive on such a site (and the warning screen) through no fault of your own you should immediately close the site and report the incident to your line manager and also helpdesk@wnc.ac.uk to have the site added to the blocked list.

7.3 Employees must not display, distribute, store or download any illegal material. Any such action will be considered as gross misconduct.

7.4 The College's Internet facilities must not be used to undertake illegal activity. Any such action will be considered as gross misconduct.

7.5 Employees must not download or distribute any pirated software using the College Internet system. Any such action will be considered as gross misconduct.

7.6 The College will retain the copyright to any material posted on the Internet by any employee during the course of his or her duties.

7.7 Employees must not use the College's Internet facilities to download entertainment software, including games, and must not play games against other opponents over the Internet, - except in exceptional circumstances following authorisation by your line manager, e.g. “The Psychology Behind Actions”, “Theory of Games Design” etc.

7.8 Any attempts to disable, defeat or circumvent any of the College's computer security facilities will constitute gross misconduct.

7.9 Whilst the College recognises employees' right to a private life, during any use of social networking sites or maintenance of personal blogs (online diaries), employees are required to refrain from making any references to the College that could bring it into disrepute, or interacting or writing on the sites in a way that could constitute harassment of a colleague, student or employer. The College will treat any breaches of these requirements as disciplinary offences.

Further information and guidance about the use of social networking sites can be found in the College’s Social Networking Policy.

7.10 The College reserves the right to withdraw at any time employees' access to social networking sites or personal blogs.

7.11 College employees must never engage in political discussions on external forums using the College's computer system.

7.12 Employees should not attempt to access any material that promotes terrorism, radicalisation or violent behaviour.

8 Copyright and Downloading

8.1 Copyright applies to all text, pictures, video and sound, including those sent by email or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

8.2 Employees are only permitted to use the designated College screensaver on College computers.

8.3 Employees are not permitted to use the College's Internet facilities to download entertainment images or videos for personal usage.

8.4 Any file that is downloaded will be scanned for viruses.

9 Responsibilities

9.1 The responsibility for drafting, updating, monitoring and reviewing this Policy belongs to the Director: IT

& Learning Resources

9.2 Employees are responsible for complying with the requirements of this Policy and for reporting any breaches of the Policy to your line manager.

9.3 IT Support is responsible for maintaining the College's computer systems. Support for employees in the proper usage of the systems is provided by a variety of sources including IT Support. Where employees require any information or help about the use or set up of the computer facilities, queries should be directed to IT Support help desk via email or telephone.
People Development provide training courses on some of the College software, contact People Development for further information.

10 **Disclaimer**

10.1 The following disclaimer is automatically attached (via a web link) to the end of every email sent externally:

Email Disclaimer

This message is sent in confidence for the addressee only.

It may contain confidential or sensitive information.

The contents are not to be disclosed to anyone other than the addressee.

Unauthorised recipients are requested to preserve this confidentiality and to advise us of any errors in transmission.

Please note that the college reserves the right to monitor emails for the business purposes contained in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

That is:

- to establish the existence of facts relevant to the business of the college, to investigate or detect unauthorised use of the systems
- to maintain the effective operation of the system
- to detect any computer viruses
- to check the mailbox of any absent employees
- to prevent or detect a crime.

To be able to exercise these rights, the college must have made all reasonable attempts to inform every person who may use the system that monitoring and interception may take place.

This college regards this notice to you as notification of such a possibility.

Any views expressed in this message are those of the individual sender, except where the sender specifies and with authority, states them to be the views of West Nottinghamshire College.