

6.11 Use of Electronic Communications

This policy sets out the rules which apply to the use of all types of electronic communications by civil servants.

- NICS rules with regard to conduct and normal standards of behaviour apply to Electronic Communications - [2. General Responsibilities of Users.](#)
- NICS Departments may monitor activity and if need be monitor the content of electronic messages - [3. Monitoring and Personal Use of NICS ICT Facilities.](#)
- Examples of unacceptable behaviour in relation to the use of Electronic Communications and the disciplinary action which will be taken – [4. Prohibited User Actions.](#)
- The implications of your actions when using Electronic Communications in an official capacity - [5. Social Media Use for Business Purposes.](#)
- Responsibilities whilst using Electronic Communications for personal use – [6. Personal Use of Social Media outside Work.](#)

The following terms within this policy are defined in the glossary:

Electronic communication, Electronic communications device, ICT, inappropriate/unacceptable material, Personal use, Smartphone, SMS/MMS, Social media.

You may also be interested in the following policies:

6.03 Discipline, 6.05 Equal Opportunities and Diversity (Dignity at work)

This policy is version 2.0

For a printable version please click the icon. Please make sure that your printed version is current with the one on this portal.

This homepage is only a guide to the policy, not the policy itself. In the event of any discrepancy between the content of this homepage and the associated policy, the wording of the policy shall apply.

6.11 Use of Electronic Communications

CONTENTS

1. Introduction	3
2. General Responsibilities of Users	4
3. Monitoring and Personal Use of NICS ICT Facilities	4
4. Prohibited User Actions	6
5. Social Media Use for Business Purposes	8
6. Personal Use of Social Media Outside Work	8
7. Copyright and Similar Issues	9
Annex A	10
Summary of relevant NICS policies	10
Annex B	11
Glossary	11

6.11 Use of Electronic Communications Policy

(Replaces Annex 9 to chapter 6.01 of HR Handbook)

1. Introduction

1.1 This policy is about the use of electronic communication. Examples of electronic communication include use of the internet, email, instant messaging, SMS/MMS or social networking. A glossary of terms is included at [Annex B](#).

1.2 The various forms of electronic communications used for business purposes enable employees in the Northern Ireland Civil Service (NICS) to communicate with colleagues, other organisations, our customers and members of the public, in a responsive, fast and flexible way. Electronic communication is therefore a crucial method by which NICS Departments can achieve their aims of transparency and accountability.

1.3 This policy applies regardless of the electronic communication device you are using. Any future devices whose functionality differs from those which are current at the published date of this policy, will be considered on their merits for inclusion within this policy. The use of electronic communication is an integral part of many civil servants' lives, but careless or negligent use can lead to complaints or legal proceedings against NICS Departments or you as an individual employee.

1.4 The rules are intended to protect the interests of the NICS, as well as the interests of users, and to ensure that individuals are not at risk of disciplinary action, criminal proceedings or civil action, as a result of misunderstanding or lack of guidance. The general principles and rules on such usage, covering users of NICS ICT facilities, are set out below.

1.5 In this policy you will see references to "inappropriate material". What this means is material that is unwanted, unreasonable and offensive and which has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment. This applies whether the material is in pictures, cartoons, words, sounds or moving images, even if it is thought to be humorous. Staff should be aware that the decision as to whether or not material is considered offensive will depend on the perception of the recipient and/or observer, rather than the intention of the sender.

1.6 At all times you must be aware of the IT security policies relating to your specific Department. In addition there are also central NICS IT security and other relevant policies which apply to all Departments. Links to these are given in [Annex A](#).

1.7 Departments publish Health and Safety policy statements which also apply to electronic communications facilities.

2. General Responsibilities of Users

2.1 As at other times, all the NICS rules relating to conduct and normal standards of behaviour apply when using electronic communication. There are a number of policies that give further guidance, specifically the [Dignity at Work Policy](#), the [Equal Opportunities Policy](#) and the [Standards of Conduct Policy](#), all of which should be read in conjunction with this policy. Links to these policies can also be found at [Annex A](#).

2.2 You should be aware that you might be **personally** liable to prosecution, and open to claims for damages, should your actions be found to be in breach of the law. In cases of harassment, a claim that you had not **intended** to harass or cause offence will not in itself constitute an acceptable defence.

2.3 As in any other work activity, you must respect the privacy and legitimate rights of others.

2.4 You will be held accountable for any misuse or breach of security, including confidentiality. Such misuse may lead to disciplinary action.

2.5 You should restrict personal use of electronic communications, whether on official NICS or your personally owned electronic devices to your own time, during non-working hours, at lunch breaks and before and after work. Your "own time" is time when you are not regarded as on official duty, or logged on for Flexi Working Hours. Other breaks (such as tea breaks or comfort breaks) that are recognised but are taken in normal working hours do not count as your own time for these purposes.

3. Monitoring and Personal Use of NICS ICT Facilities

3.1 All electronic communications on NICS ICT equipment are logged. You should note that, as is permitted by legislation, NICS Departments may monitor and review electronic communications activity, analyse usage patterns and publish resultant traffic monitoring data when this is deemed necessary for compliance or other reasons. This includes the prevention or detection of illegal activities.

3.2 Departments may also monitor the content of emails, files, instant/ text messages or other electronic communications as and when this is considered necessary in order to ensure both the integrity of NICS systems and user compliance with all of the relevant usage policies and guidance. Any attempt to disrupt Departmental monitoring could amount to misconduct or gross misconduct and may result in disciplinary action.

3.3 Users of NICS ICT resources, including electronic communication facilities, should be aware, and must accept as a condition of use, that their usage of such facilities may be monitored and should have no expectation of

privacy, whether use is for the conduct of official business or for personal use. Use of the NICS facilities for personal use will be deemed as acceptance that usage and content will be monitored.

3.4 Subject to NICS policy, and any other Departmental/Agency specific policies which may apply in relation to personal use, you may, in your own time, make use of official ICT facilities as detailed below.

You may:

- a. use internet access for personal research;
- b. use the internet for the occasional purchase of goods and services, provided payment is made by you. All delivery of items purchased should be to a private address and not to the premises of any NICS business. You must not create any contractual liability on the part of the NICS. The NICS does not accept any responsibility for the security of credit card details, or any other payment method used. Similarly, the NICS does not accept any liability for financial loss, whether as a result of fraud or otherwise, suffered while using NICS systems for personal transactions. All such use is entirely at your own risk;
- c. make occasional use of Departmental/Agency facilities for on-line banking. All such use will be at your own risk – Departments cannot accept any liability for losses or for any other liabilities arising out of such transactions under any circumstances, and
- d. make occasional use of your official Departmental/Agency email account to send, forward or receive personal emails. Such emails must be clearly marked. It is an explicit condition of using this facility that you must accept that the content of these emails may be accessed by management and/or IT staff, without notice or any requirement for consent. However, you must not supply your official NICS email address to any person, company or organisation for non-official purposes- such as registering with websites or newsletters. In these particular circumstances only a personal email account may be used. While it is not intended to undertake routine monitoring of the contents of emails (personal or otherwise), email traffic may be accessed at any time for a number of reasons. These may be to check an officer's email account for business reasons, if they are absent from work, or as part of an exercise to monitor compliance with this policy or as part of the investigation of actual or suspected security incidents.

3.5 To ensure compliance with NICS, Departmental/Agency electronic communications usage policies, Departments reserve the right to inspect and examine any and all IT equipment (supplied by NICS). These will include for example, smartphones or other mobile electronic devices used on or off official premises for the conduct of official business. Personally owned equipment **must not** be connected in any way to the NICS Network including inserting a NICS SIM into personally owned equipment to connect to

electronic communications. You should clearly understand that if you bring personal IT equipment of any nature into the workplace, including laptops, smartphones or any other electronic device, such equipment, and all data contained, may be inspected at any time if there is a reasonable suspicion that they may pose a risk to the NICS -whether by way of a virus, hacking software or the presence of improper, offensive or illegal material.

3.6. The facility for personal use is granted at the discretion of management and may be withdrawn or refused at any time for operational reasons, or if misuse is suspected or detected.

4. Prohibited User Actions

4.1 If you are found to have been involved in electronic communications-based illegal activity, the disciplinary procedures will be instigated. These procedures could result in a range of sanctions being applied which include dismissal.

The Department will fully co-operate with law enforcement authorities to identify and take action against any member of the NICS accessing, possessing or circulating child pornography. Individuals found to have been involved in any way, with possession or circulation of child pornography whilst using NICS ICT systems will face serious disciplinary action, with a probability of dismissal, irrespective of whether or not they are prosecuted or convicted under the criminal law.

4.2 In appropriate circumstances, Departments will inform and co-operate with relevant bodies in the UK such as the police.

4.3 Examples of other forms of unacceptable behaviour when using electronic communications facilities include:

- a. harassment or bullying;
- b. circulation or display of inappropriate material; for example on a screensaver;
- c. offensive remarks or comments of a sexual, racial or sectarian nature; or
- d. offensive remarks or comments regarding gender, sexual orientation, religious belief, political opinion, marital status, age, disability or dependants.

4.4 Any breach of this policy may be treated as a disciplinary matter and could be dealt with under the normal disciplinary procedures. The NICS Disciplinary Procedures can be found by clicking [here](#).

4.5 There are certain actions that could pose a substantial threat to the integrity of the NICS or its IT systems and you must be careful that you do not take these actions. They are:

- a. auto-forwarding emails from your Departmental/Agency account to personal email accounts, or from your personal email account to Departmental/Agency accounts. Emails received into a Departmental/Agency account may be forwarded once their contents have been vetted. Any forwarding of protectively marked information must comply with the NICS Guide to Document and IT Security (link at Annex A). It is recommended that you do not use private email addresses for business purposes. However, if you do, you should be aware that information held in non-work personal email accounts may be subject to the conditions of the Freedom of Information Act (FOI) 2000, including those criminal offences around the deletion or concealment of information, if it relates to official business,.
- b. knowingly spreading any type of malicious program including any virus or program designed to infiltrate a system to gather information.
- c. using NICS facilities to disable, overload, or gain unauthorised access to any computer system or network, or attempt to disable, defeat or circumvent firewalls or any NICS IT security facility intended to protect the privacy, integrity or security of systems, networks or users;
- d. knowingly connecting to any internet site that contains inappropriate material. If you accidentally access one of these sites, you must immediately disconnect from it, regardless of whether it had been previously deemed acceptable by any screening or rating program. Report the accidental access immediately to your Departmental/Agency IT support provider so that action to bar access to the site can be taken and also to safeguard you in the event of any subsequent investigation;
- e. using any NICS systems or facilities for purposes such as harassment, unauthorised public speaking, misappropriation of intellectual property or misuse of NICS assets or resources;
- f. downloading or forwarding non-business related software or data including music, graphics, videos, text, games, screensavers, wallpapers, entertainment or pirated software;
- g. using NICS facilities to play internet games, forward chain letters, or enter non-NICS approved prize winning competitions, or engage in online gambling;
- h. uploading software licensed to a Department/Agency or data owned by a Department/Agency, without the express authorisation of the manager responsible for the software or data;

- i. using NICS IT facilities to undertake trading at work (or at home) e.g. on sites such as e-bay and gumtree.

5. Social Media Use for Business Purposes

5.1 You should not comment on, or write about, the work of the NICS in the course of your NICS duties without the approval of the Principal Information Officer for your Department.

5.2 You may, with the permission of the Principal Information Officer for your Department, be authorised to make contributions to electronic communications as part of your official duties. If you have been given this authorisation, your Departmental Information Office should be contacted to answer any enquiry you may have.

5.3 Your contributions to electronic communications in an official capacity become part of the official record and are liable to disclosure under the Freedom of Information Act 2000.

5.4 As a civil servant, you must operate within the [NICS Code of Ethics](#) when engaging with electronic communications:

The Code applies to your participation online as a civil servant and sets out the core values expected of Civil Servants: integrity, honesty, objectivity and impartiality. You should participate in the same way as you would with other media or public forums, such as speaking at conferences. If you have been given permission by your Principal Information Officer to contribute to electronic communications in an official capacity, never give out personal details such as your home address or phone number.

5.5 Also be aware that contributions online may attract media interest in you as an individual, so proceed with care, whether you are participating in an official or a personal capacity. If you have any doubts, you should take advice from your line manager.

5.6 Staff should exercise the same discretion online in respect of security matters as they would anywhere else and staff who hold a security clearance must not make public or disclose on social media what level of vetting they hold. All vetted staff should keep their online profiles under review, expressly remove any reference to holding a level of security vetting and discuss any remaining doubts or concerns with their line managers.

6. Personal Use of Social Media outside Work

6.1 You should be aware that whilst using your own electronic communication device, certain behaviour in your personal capacity as a member of the public could have a detrimental impact on the NICS and may fall under the NICS Disciplinary Policy or other relevant Departmental or NICS

policies. The boundaries between work and personal life on social media can become blurred. Therefore, you need to be careful not to disclose official information without authority.

6.2 Do not bring the NICS into disrepute by your contributions to social media sites. Disrepute means online behaviour by you as a civil servant that could lead to embarrassment or cause harm to the reputation of the NICS. Articles or contributions to forums about the work of the NICS must be cleared with your Principal Information Officer. Do not comment at all on controversial issues connected with the responsibility of your own Minister.

6.3 Do not make disparaging, discriminatory or defamatory remarks about colleagues or customers who are entitled not to have their rights infringed or their reputation damaged by contributions made to electronic communications.

6.4 Do not use or disclose any protectively marked information you have obtained in the course of your NICS employment. For example, do not make reference to customers or commercial contracts. Further information on protective marking can be found in the Guide to Document and IT Security (see [Annex A](#)).

6.5 Do not make public or disclose on social media what level of vetting you hold. Keep your online profiles under review, expressly remove any reference to holding a level of security vetting and discuss any remaining doubts or concerns with your line manager.

7. Copyright and Similar Issues

7.1 Departments will, where appropriate: -

- a. retain the copyright to any Departmental/Agency material posted on any electronic communications site by you in the course of your duties; and,
- b. assume ownership of any legitimate software or files downloaded via the internet on to Departmental/Agency networks. Any such files or software may be used only in ways that are consistent with their related licenses and/or copyrights.

Use of Electronic Communications

ANNEX A

Summary of relevant NICS policies

Provided below is a list of the various NICS policies relevant to the use of electronic communications. In addition, you must also make yourself aware of any other relevant policy specific to your Department.

[ITAssist Intranet](#) (contains policy documents within site)

[NICS Guide to document and IT security](#)

[NICS Code of Ethics](#)

[Dignity at Work Policy](#)

[Equal Opportunities Policy](#)

[Standards of Conduct Policy](#)

[Discipline Policy](#)

Use of Electronic Communications

ANNEX B

Glossary

Electronic communication: Communication transmitted by means of an electronic device.

Electronic communications device: Any device that uses electronics to communicate. e.g. smartphone, laptop, tablet, desktop PC.

ICT: Information and communication technology.

Inappropriate/unacceptable material: See paragraph 1.5 and paragraph 4.3

Personal use: Any use of electronic communications facilities that is not a direct requirement of your official duties. Therefore, accessing a site for the purpose of, for example, researching social security policy or employment law developments is official use only if it is necessary as part of your work. Accessing such data for reasons which are not a requirement of your work, would be classed as personal use of the information.

Smartphone: A mobile phone that can also access the internet.

SMS/MMS: Short Messaging Service/Multimedia Messaging Service. Names given to text messages, or in the case of MMS, text messages that contain multimedia content such as pictures or moving images.

Social media: A social media site is an online facility that allows its subscribers to contribute information about themselves and take part in online communication in various forms. These forms of communication could include, but are not limited to, words, sounds, moving images or pictures.