IT CODE OF CONDUCT

The IT Code of Conduct sets out guidance on the acceptable use of SCOTS, in particular email and use of the intranet. It outlines our policy on the personal use of Scottish Government IT facilities.

The code applies to:

- anyone sending information across Scottish Government or public networks via email or internet services (including contractors and agency workers)
- users of SCOTS
- users of other IT systems or devices supplied by the Scottish Government or its agencies
- users of IT systems supplied by a third party and used for Scottish Government business

It covers:

- personal use of SCOTS and the internet
- misuse of IT misconduct examples
- accidental access to restricted sites
- sharing sensitive data by email
- monitoring

The code aligns with the wide range of legislation to tackle the potential criminal and civil liability issues that may arise from colleagues' misuse of communication facilities while at work.

You should comply with the code at all times.

You will be deemed to agree to its terms, including monitoring arrangements, unless you specifically write, stating the contrary, to:

HR Shared Services
F1 Spur
Saughton House
Edinburgh
EH11 3 XD

Personal use of SCOTS and internet

As the owner of our IT equipment, the Scottish Government is responsible for any emails and downloaded internet pages generated or stored on it.

You are allowed to use our IT facilities for personal use as long as this is in your own time, when you are keyed out of the flexi system or outside normal working hours.

Permitted use

You can use SCOTS to:

- prepare simple documents or spreadsheets on personal matters – these must not be permanently stored on SCOTS
- send brief personal emails (10 lines) with small attachments (two pages) to internal and external addresses – you must change the message sensitivity option to 'personal'
- prepare study material if you are studying for any form of qualification that is being supported by the organisation
- access the internet for personal use (excluding for reasons set out in misuse and unacceptable behaviour)

Inappropriate use

You must not use:

- SCOTS to prepare or research material in connection with running a private business
- official templates for personal documents
- chat rooms and newsgroups

All online activity is monitored. Information and Technology Services (iTECS) will inform your manager of any inappropriate or excess personal usage.

Misconduct examples – IT misuse

Misuse of IT facilities may lead to disciplinary and/or criminal proceedings.

Making defamatory, actionable or untrue statements about colleagues or contacts on email or online is no different from doing this in any other way.

Legislation that governs your use of IT at work includes:

- Civic Government (Scotland) Act 1982
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Equality Act 2010
- Data Protection Act 2018/General Data Protection Regulation
- Defamation Laws
- Copyright Laws
- Computer Misuse Act 1990

Misconduct examples

- running a personal website
- private use of chat rooms and newsgroups
- improper use of official templates
- loading any software for personal use onto your PC or laptop or network drives, including screensavers, games, CDs from a computer magazine or shareware from the internet
- subscribing to mailing lists ('listservers') for purposes other than those that are work-related
- inserting personal removable media into a SCOTS device (e.g. memory sticks, CDs, DVDs, etc.)

This list is not exhaustive. Each case will be considered on its own merits, but may lead to disciplinary action.

Examples of serious disciplinary offences

- attempts to access, active accessing, downloading, display, storage and distribution of pornographic, racist or other offensive material, or material relating to illegal activities
- disclosing your SCOTS password to someone else to use
- attempting to access and gaining access with the intent to modify data or programs in parts of the SCOTS network for which you don't have authorisation. These are also criminal offences.
- generating messages in a way that makes them appear to come from someone else
- sending abusive, offensive, libellous or nuisance emails
- generating and/or distributing chain email
- using IT facilities for private commercial use

- contravening the rules of personal use of IT facilities
- distributing or printing copyright materials in violation of copyright laws
- participating in user groups or discussions which are politically sensitive or potentially controversial
- use of any system supplied by a third party for purposes other than it was supplied for

This list is not exhaustive. Serious offences could lead to dismissal for gross misconduct.

Accidental access to restricted sites

It is possible to connect accidentally to websites that contain illegal or offensive material.

If this happens to you, you should disconnect from the site immediately and inform your manager.

If you receive an email which you consider may contain pornographic or offensive material, you should close the document, advise your manager and telephone the IT Helpdesk on 0131 244 8500 (option 2).

Sharing sensitive data by email

You should never send sensitive information to cabinet secretaries or ministers outside the Scottish Government in an external email or over the internet.

Personal email addresses must not be used to register for business services. All information services and assets must be registered in the information asset register.

You must use the Public Services Network (PSN) to send mail to other government departments for documents up to and including OFFICIAL-SENSITIVE.

If in doubt about whether material is regarded as sensitive, email cyber security and defence for advice on how to share it.

Monitoring use of IT systems

We monitor and regularly review the use of our IT systems.

We record:

- all email activity
- the user name, PC, date and time and full address of every internet site accessed (even if the attempt is unsuccessful)

You should be aware that many internet sites record visitors for marketing purposes, and this information could become public.

As part of our standard monitoring procedures, we will raise any evidence of misuse with Information and Technology Services (iTECS) and People Directorates.

Contact HR Help if you are:

- a manager who is concerned about one of your colleague's use of IT facilities – you should first raise any issues with the colleague
- concerned that a colleague is misusing the system or that your PC has been misused