Information Governance Good Practice and Email Etiquette

Remembering passwords:
Choose passwords you can remember without having to write them down. For example you can the first letter of each word in a phrase, include capital letters and numbers in your password – but make sure your passwords are 'strong' and store them in a safe and secure location.

Always use your own login when accessing systems:
If you use someone else's login and password it is difficult to tell who did what. Protect yourself by always using your own login and never share your password. You are responsible for ensuring that your password cannot be accessed or used by somebody else.

Lock your PC/Laptop when it is unattended:
Many information security breaches are opportunistic. Press the 'Windows' button and 'L' at the same time, or press 'Ctrl', 'Alt' and 'Del', then select 'Lock this computer' to lock your screen even if you have to leave the PC for a few seconds.

Keep out of sight!
Keep work-related documents notes, diaries and equipment such as laptops, tablets and smartphones out of sight e.g. lock in drawers or in car boots when unattended.

Keep printouts secure:
Collect prints from printers as soon as you can to avoid them being read / misplaced by other people and used 'Locked prints' where possible..

Keep confidential information held on paper safe and secure until disposal:
Store it separately in a locked drawer / cupboard and dispose of it by shredding.

Don't open emails sent from senders you don't recognise:
They often contain malware such as Viruses. To avoid being targeted delete these emails, especially if they contain attachments.

Check Recipient Names:
Use 'Check Names' to confirm which health board/authority your email will be sent to before you send it. The health board/authority will appear in brackets after the recipient's name.

Use 'To:' and 'Cc:' correctly
Only include people in the 'To:' field whom you expect to read and respond to the email. The 'Cc:' (Carbon Copy) field should be used for people you want to know about the email but you are not expecting a response from them, i.e. to keep them in the loop.

Take care when using 'Reply to All':
When sending a 'Reply to All' be aware that it will be sent to everyone who received the email, including those who were copied into the original email and ask yourself if they really need to see the correspondence.

Email isn't private
Remember email isn't private and may be subject to disclosure under Data Protection and Freedom of Information (FOI) Legislation. In addition don't put anything in an email you wouldn't be prepared to defend in court.

Put your contact details at the bottom of the email.
It's good practice to put your contact details at the bottom of the email. That way you can be contacted by the recipient(s).

Double-check before you press 'Send':
Do a visual check before you send the email. It's easy to make mistakes so it's a good idea to re-read emails and make sure that address(es) are correct, there are no spelling mistakes, the message is clear and that good email etiquette has been observed

If in doubt, ask:
If you are unsure about an email address ask someone, don't guess. The IT department is available to assist.

Fairwarning Privacy Breach Detection Software

To assist Health Boards in continuing to keep patient information secure and confidential all Health Boards have been issued with Privacy Breach Detection software known as FairWarning.

FairWarning, can be linked to all of our clinical and staff computer systems and can analyse activity on our clinical systems and report on instances where potentially inappropriate access has occurred. Examples of this include users looking up records of colleagues, family members, neighbours or even their own records.

The introduction of FairWarning does not mean any changes for staff. It has always been a condition of employment that access to clinical records is on a strictly need-to-know basis. The Information Governance Code of Conduct, along with the Confidentiality Statement that every member of staff is required to sign, reiterates this. FairWarning is simply the means by which we can assure our patients, the Board and the Information Commissioner that the information we hold is handled correctly and in accordance with the law.

If a member of staff wants to view their own health records, or those of a dependent relative, they must follow the same process as any member of the public, i.e. the Subject Access Request process as stipulated in the Data Protection Act 1998

Line Managers will be sent a report if FairWarning identifies any *potentially* suspicious activity that has been performed by a member of staff. The type of activity that may generate a report includes, but is not restricted to, viewing their own record or that of a member of their family, a neighbour or a work colleague. If you, or any member of staff, has a specific concern about who may have been accessing a particular health record a tailored report can be produced.

Staff member accessing own record(s)

If a staff member accesses their own record, the manager will arrange to meet with the member of staff and explain why this is a breach of NHS Orkney's Information Security Policies and inform the staff member that any further breaches may be dealt with in line with the NHS Orkney Management of Employee Conduct Policy.

The manager will also complete a DATIX form to formally record this breach of Information Governance / Patient Confidentiality.
Formal action may be taken as a result of a staff member accessing their own record.

Staff member accessing someone else's record(s)

If there is no work related reason for the staff member to access the clinical records, the manager will ask for a more detailed report of the staff member's electronic activity over an appropriate reference period, e.g. three months, to ascertain whether there have been any further breaches. The manager should also complete a DATIX form to formally record this breach of Information governance / Patient Confidentiality.
When the detailed report has been obtained and analysed the manager should contact the Human Resources Department to arrange an investigatory meeting with the member of staff in line with the NHS Orkney Managing Employee Conduct Policy.
If there is historical evidence that the staff member has inappropriately accessed patient records and they are unable to provide a satisfactory explanation, a decision may be taken to refer the case to a disciplinary hearing in line the NHS Orkney Management Employee Conduct Policy.

Staff member shares information only they can know with a third party

In the event that a member of staff is suspected of sharing any information with a third party, a full investigation should be carried out in line with the NHS Orkney Management of Employee Conduct Policy.
Where the balance of probability indicates that patient information has been shared or disclosed to a third party, this is likely to constitute gross misconduct which would usually result in termination of employment.

The security of patient data within health authorities has been given a high profile in recent years and the Information Commissioner's Office now has increased powers, including the power to fine organisations up to £500,000 for serious breaches. The negative effect on the organisation's reputation would have an even greater impact than a monetary fine.