



Information Commissioner's Office



Personal use of computers



Personal use of computers

CONTENTS

	Page
BACKGROUND	3
ACCEPTABLE USE.....	3
MONITORING	5
ACCESS.....	7

Personal use of computers

Background

In addition to the internal mail system, ICO staff have direct access to the Internet and external email from their desk and laptop computers.

This statement of the Commissioner's policy on what is acceptable personal use of computers by his staff lays down general rules and gives examples of what those rules represent. If you consider that your personal use of your computer would fall outside these guidelines, you should ask for authority from your manager to do this.



Acceptable Use

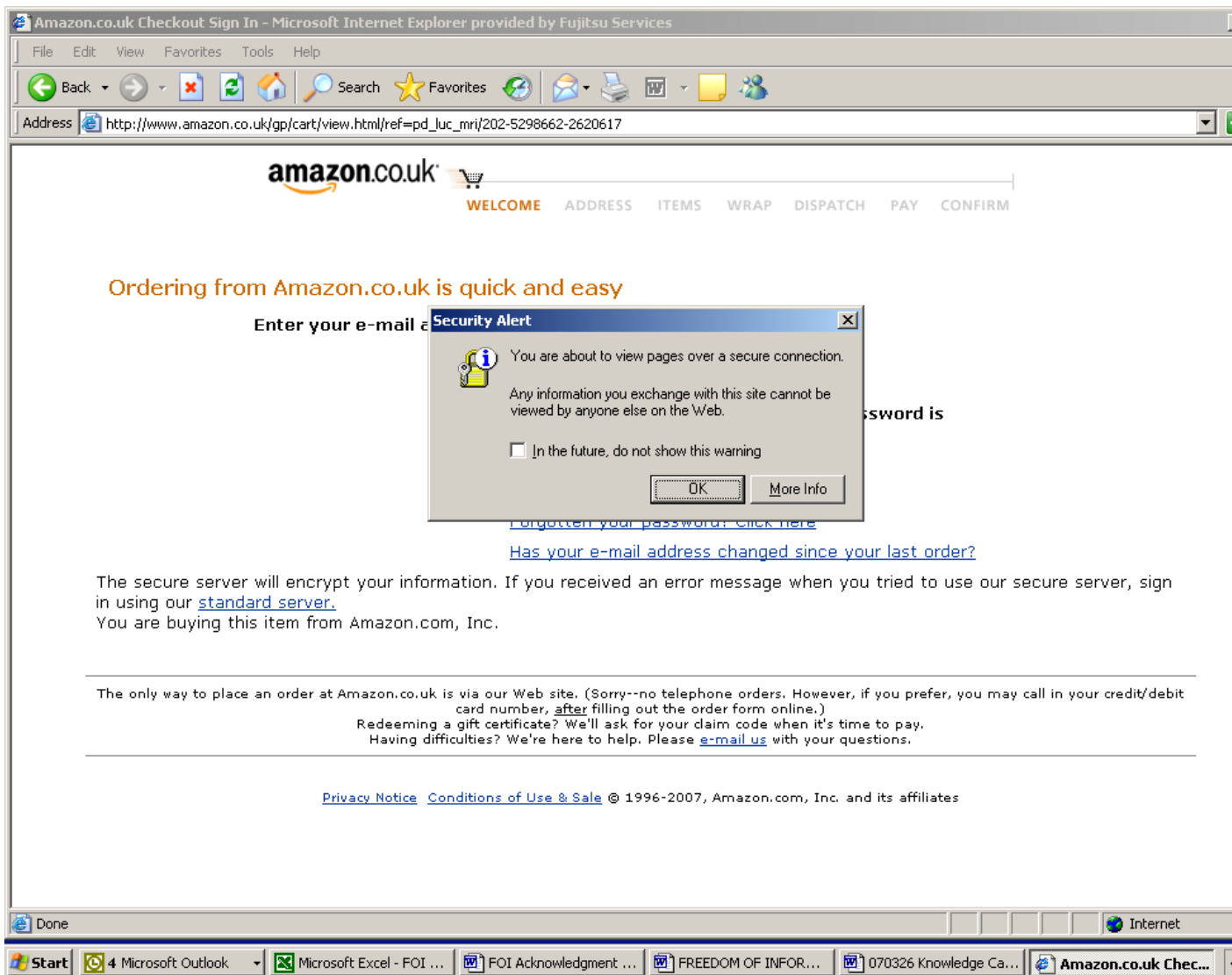
The ICO computer system exists to support the business purposes of the office.

Computers are provided to members of staff to carry out authorised business functions. The equipment should not be used by anyone other than a staff member or someone authorised to act on behalf of the Commissioner.

The Commissioner recognises that some personal use, including use of the Internet and external e-mail, will occur. This should only occur when computers are not needed for office work, out of core times and when you are keyed out. It is also accepted that some limited use of the internal e-mail system for personal purposes may occur in normal working hours. Nevertheless, as a generality, personal use should not be frequent or excessive.

The following points should be noted:

- You must not access any website built with a secure connection for **personal use**. The risk to ICO is that if connections to HTTPS sites are permitted via these secure links, the content of the connection is invisible to our firewalls. This could mean that virus's or malicious code could go undetected from an unknown source and could infect not only our network but also the wider GSi community. You will know if you are accessing a site, or part of a site, of this nature as you will be notified by a pop up box, as shown below, explaining that you are about to connect via a secure connection. At this point you must close the pop up by clicking on the cross in the top right hand corner and proceed no further.



Access to these sites for personal use should only be from the stand alone computers within the office. However, it is accepted that access to these sites will be needed for business purposes and in these circumstances the networked pc's can be used.

- The purpose for personal use should be limited, for example, you must not use the Internet to conduct transactions on-line, however you can use it to research topics of personal interest.
- You must not use office computers or services for outside business interests; however it would be acceptable to prepare letters, use a spreadsheet or prepare other documents for personal use.
- Whilst the Commissioner recognises that you will not always be able to stop a personal e-mail from being received, external personal e-mail should not be encouraged, for example, by giving out your business e-mail address to personal contacts or signing up for e-mail alerts. External e-mails should only be sent occasionally and out of core hours. Any personal external e-mail should be short with no large attachments such as photos. Any personal e-mails you do send should be marked in the subject box "Non Work".
- You must not access private e-mail accounts (such as Hotmail & Yahoo) from office computers unless you have been given authority to do so.
- Personal usage should be within the bounds of the law and decency. You should ensure appropriate courtesy and respect to others. You should not, for example, use your office e-mail address to express your personal views on issues which may be seen to be related to the office since such use could extend liability for those views to the ICO. Disparaging remarks about others should not be made.
- For the avoidance of doubt, no sexually explicit or racist material, indecent images of children or any material likely to cause offence or embarrassment to others should be created, downloaded or accessed.
- You should only visit chat rooms directly related to work purposes, such as Data Protection and Freedom of Information.
- If you download data from the Internet, you must use the virus checking process. This is explained in the Users Guide to Security which can be found on ICON.

Laptops

This policy applies to the use of ICO laptops even when used outside the office.



Monitoring

Because some limited personal use is anticipated, you need to be aware that use of any computer, including which websites have been visited and when, and information about external and internal e-mail traffic, including that marked “Non Work”, will be monitored and, potentially, will come under scrutiny. This means that if you have used an office computer for personal use, this will be included.

The Commissioner does not want to interfere in the personal lives of his employees but monitoring of a secure network is necessary as is use of office equipment. There is also a legitimate business purpose in checking on the use of office time. It is sensible advice to point out that when you use the office computer equipment for personal purposes you should do only those things you would not mind your employer knowing about.



It should be noted that the office does not currently monitor the content of e-mails as a matter of routine. However, it should also be noted that, where there is reason to believe that the law or office policy or procedures have been broken, the content of e-mails may come under scrutiny. The office will take into account the fact that an e-mail has been marked “Non Work” in the monitoring or investigation it undertakes and, where it is possible and appropriate, examination of this material will be avoided.

The activity on the system which will be audited for the purposes of compliance with this policy include:

- All Internet use will be logged to display date, time, username and target URL (the website visited);
- All attempts to access blocked sites

- Top 40 users by browse time
- All e-mail use will be logged to display date, time, username; and the address to which the message is being sent
- All remote access to the ICO network will be logged to display the date, time and user name of all users accessing the service.

An activity report will be produced by the Security Team for all Departmental Heads on a monthly basis. This report will show browse time for members of staff within that department only.

If misuse is suspected, an investigation will take place and this may result in disciplinary action. Disciplinary procedures will adhere to those laid down in the staff handbook. All audits and logs will be retained for a year.

Additional audits or monitoring may be activated in the system with the agreement of the Departmental Security Officer (DSO) and the Human Resources Director..



Access for Information Request Compliance

If you intend to keep copies of non work related e-mails or other documents on your computer, you should give thought to the possibility that they may need to be made available if the office receives a subject access request or a request under the Freedom of Information Act.

When you are asked to search your system in response to such a request, you should include non work related documents and emails in your search. This may mean that you will choose not to keep records of these documents on the system. You should be aware that even when documents are deleted they can still be held as part of our back up procedure for up to 16 days.

If you have any doubts whether or not this information should be included you should seek advice from your manager or the person to whom the request has been allocated.

Members of staff are given the opportunity to have 'Private Working Folders' on their system. For the avoidance of doubt, you should be aware that these folders may need to be accessed either for work purposes or to fulfil statutory requests for information such as a subject access request. This would only be done if the member of staff concerned were absent from the office at the relevant time and could not therefore access the information themselves. Again e-mails that are marked 'non work' will not be opened unless it is unavoidable.

This policy may be subject to change, in which case you will be issued with a new version.

