

Resources

ICT Services

Personal Information Security Policy

Altogether better



Contents

- i.* [Glossary](#)
- 1. [Introduction](#)
- 2. [Acceptable Use of ICT Equipment](#)
- 3. [Internet Usage](#)
- 4. [E-Mail Usage & Data Sharing](#)
- 5. [Telecommunications](#)
- 6. [Access to Systems](#)
- 7. [Security of Equipment and Information](#)
- 8. [Information Security Incidents](#)
- 9. [Social Media and Online Participation](#)

Appendices

- 1. [Email Management Guidelines](#)
- 2. [Safe-Haven Guidelines](#)
- 3. [DCC ISMS Document Set](#)
- 4. [Metadata and Change History](#)

i. Glossary

BPSS: Cabinet Office employee screening standard used for anyone working within or on behalf of a government department.

BYOD: Bring Your Own Device. The practice of allowing employees to use their own computers, smartphones, or other devices for work purposes.

Data Sharing Agreement: An agreement to ensure that sharing of personal or sensitive data is in accordance with the DPA. Particularly relevant where sharing is systemic, large-scale or risky. Further guidance can be found on the intranet or within departmental-specific policies.

DBS: Disclosure and Barring Service. Helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups. Supersedes Criminal Records Bureau (CRB) checks.

DCC: Durham County Council.

DPA: Data Protection Act 1998

Note: The DPA will be superseded in 2018 by the General Data Protection Regulations

GCSx e-mail: A secure e-mail system allowing the exchange of sensitive data between DCC and other public sector organisations.

ICO: Information Commissioner's Office

ICT: Information and Communications Technology (or the department within DCC Resources bearing that name)

Internet Gateway: The combination of hardware and software enabling DCC staff to gain secure access to the internet.

IS: information security

ISMS: Information Security Management System

Juniper/Pulse: Dual-factor authentication method used to secure remote access connections to DCC systems. Used both for staff and third-party connections.

Malware: Malicious software, designed to: disrupt the operation of computer systems; gain unauthorised access; gather sensitive information; or some other undesired outcome.

Patches: regular, interim software updates to computer systems. These can cover both functional improvements and essential security updates.

Personal information: Information that can be used to uniquely identify, or can be used with other sources to uniquely identify a single individual.

PIN: Personal Identification Number (for example, as used to secure a mobile phone)

PSN: The Public Services Network is a “network of networks” across the UK public sector, operating to an agreed set of compliance standards and management controls. It enables authorities across the UK to share information securely with local government and central government departments and agencies.

PSN CoCo: *PSN* is managed by the Cabinet Office and annual Code of Connection compliance submissions (CoCo submissions) are assessed by them. Failure to meet the compliance requirements can result in critical council services being disconnected from the *PSN*.

Sensitive information: Information which includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual life
- commission of offences or alleged offences

SIM: Security Identity Module (removable card found within mobile phones)

SMT: Senior Management Team

Unauthorised Devices: Devices that have not been supplied or sanctioned for use by DCC.

1. Introduction

- 1.1 The purpose of this policy is to assist in the protection of all data and information assets owned and used by DCC employees (temporary or permanent), elected members, contractors, agents and anyone else processing information on our behalf from the risks posed by inappropriate use. This includes protecting equipment and information from unauthorised or unlawful access, accidental or deliberate loss, damage, theft, disclosure or destruction.
- 1.2 This policy explains what our expectations are when our computer equipment is used and our information is accessed.
- 1.3 Your actions are vital in ensuring the security of customers' information.
- 1.4 It is the **personal responsibility** of all employees (temporary or permanent), elected members, contractors, agents and anyone else processing information on our behalf to comply with this policy and keep our equipment and information secure. Agency workers and sub-contractors who are required to use DCC's systems should also be made aware of, and will be expected to comply with this policy.
- 1.5 Any deliberate breach of this policy could amount to a criminal offence under, for example, the Computer Misuse Act 1990 and the Data Protection Act 1998. All incidents will be investigated and action may be taken under DCC's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and/or criminal action being taken
- 1.6 The principles described within this policy apply equally to all information held on any type of medium; whether electronic, paper or other (e.g. microfiche, audio or video).

Training

- 1.7 The dissemination of this policy is supported by training, available to all staff through the corporate e-learning system¹. Completion of the training will be recorded and monitored.
- 1.8 Reference to this policy is incorporated within employee induction.

Disclosure of Information

- 1.9 Personal or sensitive business information held by DCC can only be disclosed, whether internally or externally, when the person holding the information is fully satisfied that the requester is authentic and is legally entitled to the information.
- 1.10 The disclosure of *personal information* is subject to the Data Protection Act.
- 1.11 For more general requests for information held by DCC, the Freedom of Information Act (FOIA) applies. Where this information relates to environmental matters, the Environmental Information Regulations (EIR) apply².
- 1.12 Particular restrictions apply to payment cards. Card numbers (Primary Account Numbers) must not be written down, communicated electronically or disseminated by other means.

Guidelines

- ¹ DCC Learning Nexus system
- ²Consult the Information Management team (IMT) for clarification on any information disclosure issues. Further guidance can be found on the IMT intranet site.

2. Acceptable Use of ICT Equipment

- 2.1 DCC ICT equipment, systems or information must not be used while working for another employer, your own company or for personal political purposes.
- 2.2 Responsible personal use of DCC ICT equipment is permitted during your own time¹.
- 2.3 The use of electronic storage must be reserved for DCC business use; our storage systems have a significant cost attached and its use for personal or private purposes will be seen as an abuse of resources². DCC ICT reserves the right to delete files of a personal nature³ found on DCC resources in order to protect service delivery - potentially without prior notice. Files of a personal nature will not be restored from backup.
- 2.4 Off-site use of DCC laptops and tablets, where a DCC network connection is unavailable, is only permitted in the following circumstances:
- The device is updated with the latest *patches*
 - Before using the internet or DCC network, you must log into *[removed]* (Dual Factor Authentication) to secure your connection
 - You follow the requirements listed in the *Mobile Working* section of this policy
- 2.5 ICT Services maintains a list of approved software applications. If you have a business need to use something that isn't currently installed on your device, you will need to raise a request through the ICT Service Desk.
- 2.6 DCC logs ICT systems usage. In the event of suspected misuse, management can request logs from Internal Audit in accordance with the *Request for Access to Electronic Data* guidance notes (available on request).
- 2.7 DCC systems incorporate numerous security mechanisms, which protect both the systems and the staff using them. It is essential that the integrity of these is maintained at all times. If problems arise, contact the ICT Service Desk for assistance.
- 2.8 Usage of, and access to, DCC ICT equipment by third parties is subject to the Third Party Access Policy.
- 2.7 Any loss of ICT equipment must be reported promptly to your line manager⁴ and a call logged with the ICT Service Desk.

Guidelines

- ¹Your own time is that which falls outside the hours that you are clocked-in for.
- ²In particular, personal media files have a major impact on our storage capacity. For example, photos, music and video material.
- ³It is important to remember that ICT equipment remains the property of DCC, whether it is used for DCC business or personal use.
- ⁴Line managers have the responsibility to report the loss of ICT equipment as outlined in the data breach procedures within the DCC Data Protection Policy.
- The security of DCC ICT equipment is dependent on your actions and behaviour.

3. Internet Usage

- 3.1 DCC encourages business use of the [DCC website](#) and the wider Internet to help us maximise our efficiency and effectiveness. The Internet must be used for lawful purposes only and you must comply with relevant legislation¹.
- 3.2 DCC Internet provision must not be used to access any inappropriate² material. Take particular care when downloading; if in doubt, consult the ICT Service Desk.
- 3.3 Internet access for personal use is at DCC's discretion and must not affect your performance or productivity at work. Any misuse of this facility can result in it being withdrawn and could result in disciplinary action.
- 3.4 Access to a selection of websites and web applications is automatically blocked, based on corporate rules³. If there is a business need, access can be selectively granted by raising a request with ICT Service Desk.

Guidelines

- ¹Acts of particular relevance include:
 - [Computer Misuse Act 1990](#)
 - [Data Protection Act 1998](#)
- ²Inappropriate material includes, but is not limited to, anything that might be considered:
 - racist
 - sexist
 - defamatory
 - sexually explicit
 - gambling-related
 - offensive
 - illegal
 - trading sites; particularly with regard to running your own business
- ³Certain sites, and types of site, are restricted by the DCC *internet gateway*. However, this isn't infallible so if any inappropriate sites are not yet restricted, this should not be seen as implied consent.
- If you inadvertently access inappropriate material, this should be reported to the ICT Service Desk. This will enable ICT to block future access to such sites and will provide mitigating evidence that your access was inadvertent.

4. E-mail Usage & Data Sharing

4.1 The standard corporate email system offers only minimal protection for emails being sent externally. Where the content of an email includes personal, sensitive or otherwise confidential information, the most appropriate methods should be selected in line with the level of risk¹.

4.2 E-mails bearing personal or sensitive information must only be sent to recipients who have the need and right to access it. Employees' personal email accounts must not be used as a means of sharing or transmitting confidential DCC business information.

Email auto-forwarding must not be used as this can result in inadvertently sending personal or sensitive information to a non-secure address.

4.3 For exchanging personal/sensitive information with other public sector organisations, *GCSx email* accounts are available. *GCSx email* accounts can be requested by contacting the ICT Service Desk. The approval process follows *BPSS* guidelines and involves *DBS* checking.

4.4 For exchanging personal/sensitive information with organisations outside of the public sector, *egress* secure email is available. *egress* accounts can be requested by contacting the ICT Service Desk. Further guidance is available on the *egress* intranet page.

4.5 It is your responsibility to ensure that you use the correct addresses in your e-mails – especially those including personal or sensitive information. In the event of you mis-addressing such an e-mail, you must report it to your line manager as a potential data breach².

Similarly, if you *receive* a mis-addressed e-mail containing personal or sensitive information, you should report this to your line manager as a potential data breach. You must not forward a mis-addressed email to other recipients as this will worsen the potential data breach.

4.6 Email distribution groups also present risks of mis-addressing email. If you find that you are part of a group that you shouldn't be, contact your ICT representative. If you are responsible for an email group, ensure that you regularly maintain its membership.

4.7 If you suspect that an e-mail you receive contains *malware*, report it to ICT Services immediately by following the spam reporting process. Such e-mails must not be forwarded to anyone.

4.8 Usage of your DCC e-mail account for personal use is at DCC's discretion and must be within your own time.

4.9 Your e-mail account has a finite storage limit and is not designed to be a filing system. You must manage your e-mails so that important information is retained in appropriate storage areas and in compliance with corporate retention guidelines (see Appendix 1 for e-mail usage guidelines).

Monitoring

4.10 DCC maintains logs of e-mail traffic. In the event of suspected misuse, management can request logs from Internal Audit in accordance with the *Request for Access to Electronic Data* guidance notes (available on request).

(continued overleaf)

4. E-mail Usage & Data Sharing (continued)

- 4.11 Your e-mail account can be accessed by line management in circumstances where there is a business need to do so. For example, in the event of sickness or leave.

Regular Online Data Sharing

- 4.12 Regular, large-scale sharing of personal or sensitive information with third parties should only take place where there is a valid *Data Sharing Agreement* in place.
- 4.13 Any system used for sharing personal or sensitive information must comply with the DPA. Key points include:
- The data must be encrypted to an appropriate level
 - The servers that store the data must be hosted within the EU
 - There must be a valid contract between DCC and the online storage provider
- 4.14 Corporately approved systems are available for securely sharing information. If in doubt, consult the ICT Service Desk.
- 4.15 Any information shared through online systems should be deleted as soon as the need for sharing has passed.

Guidelines

- ¹Solutions are available for the secure transfer of information, depending on its sensitivity and the assessed risk. Further guidance is available from ICT Service Desk.
- ²The “Recall This Message” function cannot be relied upon for external emails, so the potential breach should still be reported.
- Information can be shared, when appropriate, by the use of shared folders on the DCC network or by document management systems such as Sharepoint.
- In the event of a data breach, the emphasis will be on resolving the breach and preventing reoccurrence, rather than apportioning blame.
- The **Internet Usage** section of this policy contains further guidance on what constitutes inappropriate material.
- The DCC e-mail gateway is capable of blocking viruses and inappropriate content. If any such material gets through, this should not be seen as implied consent.
- Care should be taken when using DCC email addresses for personal business – especially if there is risk of exposure to reputational damage.
- Any e-mail monitoring will be in accordance with the **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**.

5. Telecommunications

Telephones & teleconferencing

- 5.1 Conversations involving sensitive information should be conducted discreetly and, where possible, in private. Personal data should only be given where there is a business need to do so and the identity of the other party is certain.

Mobile phones

- 5.2 All DCC mobile devices must be acquired through the DCC corporate contract.
- 5.3 DCC mobile phones must have both their *SIM* and voicemail *PINs* enabled and set to something other than their default setting.
- 5.4 Business data should only be stored on a mobile phone if there is a genuine business need and should be deleted as soon as that need has ended.
- 5.5 Outgoing mobile phone call records are logged. In the event of suspected misuse, management can request logs from Internal Audit in accordance with the Request for Access to Electronic Data guidance notes (available on request).

Faxes and Multi-Function Devices (MFDs)

- 5.6 Fax machines should only be used where there is no better alternative. Where the third party has no alternative method of their own, receipt from, or sending to their fax equipment can be achieved through DCC's electronic fax system¹
- 5.7 The sending of faxes containing *sensitive or personal information* must be conducted in line with Safe-Haven guidelines (see Appendix 2).
- 5.8 Fax machines, MFDs and related equipment must be disposed of securely. Contact the ICT Service Desk for assistance.

Guidelines

- ¹The corporate fax system is *[removed]*. For further guidance, please refer to ICT Service Desk.
- For further guidance on dealing with *sensitive or personal information*, consult the DCC Data Protection policy.
- Further guidance on the use of mobile phones can be found within the Mobile Phone Usage intranet page.
- Further guidance on the use of mobile ICT equipment can be found in the **Mobile Working** section of this policy.
- The correct disposal of faxes, photocopiers and MFDs is particularly important as many such devices contain hard-disks for temporary storage. Sensitive or personal data can be extracted from these hard-disks if they aren't appropriately disposed of.

6. Access to Systems

- 6.1 Your permission to access DCC systems will only be granted when verified by a formal request by your line manager.
- 6.2 You must only attempt to gain access to systems which you have authority to use, using the credentials that have been assigned to you.¹
- 6.3 All users of DCC systems are given a Username and Password; these are unique and must be kept secret. You must not share your password with anyone and you will be held responsible for all activity using your credentials. All passwords must conform to the following specification:
- [removed]
- Using the above rules², you should aim to construct a password that is complex but memorable. Passwords are periodically monitored for quality.
- There must be a maximum of sixty days between password changes.
- 6.4 The data that you have access to when using DCC systems must be handled in line with prevailing Data Protection policy and legislation.
- 6.5 Information created or collected during your work for DCC remains the property of the Council. Such information can be accessed by management in circumstances where there is a business need to do so.³
- 6.6 DCC maintains logs of ICT systems usage. In the event of suspected misuse, management can request logs from Internal Audit in accordance with the *Request for Access to Electronic Data* guidance notes (available on request).

Guidelines

- ¹It is an offence under the **Data Protection Act 1998** to unlawfully obtain, disclose or procure the disclosure of personal data without the permission of the data controller. It is also an offence to sell personal data obtained in these ways
- ²Refer to DCC intranet for the latest password guidance.
- ³Your absence shouldn't get in the way of carrying out the business of the Council, hence the potential need to access your information in your absence.
- Anything stored on DCC systems can be disclosable under a Subject Access Request (Data Protection).
- In managing information as part of your duties, the preference should be to store it within a specific business system or a shared storage area (such as Sharepoint).
- There should be no expectation of personal privacy on DCC systems. It is therefore advisable not to store private material on DCC systems.
- Signing up to the self-service password reset system will help in the event that you forget yours.

7. Security of Equipment and Information

- 7.1 Whenever you leave your workstation, you must lock your computer¹.

- 7.2 All personal and sensitive business information must be locked away when unattended and not left on desks.²
- 7.3 When *sensitive or personal information* needs to be disposed of, this should be done securely in a manner that prevents the information being accessed or reconstructed. Retention of information must be in line with DCC Records Management Policy.
- 7.4 You must not connect (either physically or wirelessly) *unauthorised devices* (including mobile phones, laptops and tablets) to DCC ICT systems; DCC does not permit *Bring Your Own Device (BYOD)*. DCC business information must not be transferred onto *unauthorised mobile devices* or media.

Guidance for the usage of memory devices can be found in USB memory stick usage.

Asset Tracking & Disposal

- 7.5 When ICT assets are provided, they are logged and monitored. If transferring equipment to another member of staff, notify ICT service desk to update the register. Refer to the Physical Asset Control policy for more details.
- 7.6 For the destruction of paper-based information, you must use the corporate secure shredding bins. Contact the Information Management team if none is available.
- 7.7 For electronic media bearing personal or sensitive information, the corporate secure shredding facility should be used.³
- 7.8 For the secure disposal of electronic equipment or media, contact the ICT Service Desk.

Mobile Working

- 7.9 Any mobile computing device bearing personal or sensitive information must be encrypted using methods approved by DCC ICT Services. All available security mechanisms should be enabled and no attempt made to bypass them.⁴
- 7.10 Mobile computing equipment must be kept secure at all times, out of sight of opportunistic thieves. Whenever such a device is taken outside of a secure DCC office environment, every reasonable effort should be taken to minimise the opportunity for loss, theft or damage.⁵
- 7.11 In public areas, take precautions to ensure that personal or sensitive information can't be overlooked by passers-by.

Paper-Based Information


- 7.12 This policy applies equally to information held on paper files and any other medium on which it is held. You should review the corporate Records Management Policy and the corporate Data Protection Policy regarding the use of paper records containing *sensitive personal information*.
- 7.13 When the need for taking paper records out of the office arises, consult the *Secure Handling and Transit Guidance*.

(continued overleaf)

7. Security of Equipment and Information (continued)

- 7.14 When it is essential to post paper-based information, consideration must be given to using registered or other secure mail services, depending on the sensitivity of the information.

Guidelines

- ¹To lock your computer temporarily, you must hold down the keys  + L at the same time. When you want to close your computer down, use *ShutDown*, rather than *Standby* or *Hibernate* modes.
 - ²Where it isn't possible to be in proximity of your ICT equipment, you should avoid it being left on view in vehicles, public transport or any other public space; left unsecured on desks overnight; or left in vehicles overnight. Always use the most secure methods available to you at any given time.
 - ³There is a corporate contract with [removed] for the secure shredding of confidential waste. Tel. [removed] or email [removed]
 - ⁴Different devices have different capabilities, so you should take time to understand how yours works and what this means for the security of the information it contains. For encryption, our *PSN* compliance depends on us employing appropriate encryption to data at rest and in transit.
 - ⁵When leaving a portable computing device in your (non-DCC) vehicle is unavoidable, DCC insurance cover applies if all of the following conditions are satisfied:
 - The equipment must be locked in the boot of the vehicle
 - All doors are locked
 - All windows and the roof are closed and fastened
 - All security devices are put in full and effective operation
 - All keys or any other removable ignition device of the vehicle are removed.
 - If equipment is to be left in the boot of a vehicle, the vehicle must be parked in a well-lit area/carpark, not in a remote area.
 - The equipment must not be left in an unattended vehicle for more than 4 hours.
 - The equipment must not be left in an unattended vehicle overnight even if the vehicle is garaged.
 - All reasonable steps should be taken to protect information. For example, where information needs to be taken outside of the office for work purposes:
 - If a device or paperwork needs to be left at home overnight, protect it in the most secure manner available. If a locked cupboard is available, use it. Alternatively, ensure it is out of sight and that there is nothing visibly to suggest it being there (e.g. laptop bag).
 - In the case of transporting information from site to site, consider carefully whether you can avoid leaving information behind in your vehicle. If not, ensure it is either locked in the boot or obscured from view.
- More detailed guidance available in *Secure Handling and Transit Guidance*
- If you regularly need to print *sensitive or personal information*, consult the ICT Service Desk for advice on the most secure printing solutions.
 - All of these policy statements apply equally when you are working from home.
 - Breaches of information legislation are monitored and remedies enforced by the ICO. More information can be found at their website: <http://www.ico.org.uk/>
 - The intranet site for the Information Management team, including associated policies and guidance can be found here: [removed]

8. Information Security Incidents

When any of the eight principles of the DPA are not complied with, a data breach is considered to have occurred. The procedure for responding to such a breach is contained within the Data Protection Potential Breach Procedure. If that breach involves an ICT device or service, ICT Services will invoke the Security Incident Management Procedure ([SIMP](#)).

- 8.1 It is the responsibility of all members of staff to maintain vigilance about the security of information and to report any suspected incident. Where an incident is identified that affects an ICT asset, it must be reported to the ICT Service Desk.
- 8.2 The SIMP describes ICT Services' actions in resolving incidents that impact on ICT assets through the following stages:
 - Detection
 - Containment
 - Eradication
 - Recovery
 - Lessons-learned
- 8.3 Where an IS incident involves a breach of personal or sensitive data, the Data Protection Potential Breach Policy will be invoked¹ at the earliest opportunity.
- 8.4 On completion of the investigation of high-priority incidents, there will be a Post-Incident Review. Findings will be reported to ICT *SMT* and, where appropriate, fed into the Data Protection Potential Breach Procedure.

Guidelines

- ¹General data breaches should be reported to *[removed]* in line with the Data Protection Potential Breach Policy.
- Our approach to IS incidents is vital to the maintenance and continuous improvement of our *ISMS*. The lessons we learn from incidents are used to improve our policies, processes and practices. Examples include:
 - denial-of-service attacks; network monitoring alerts; website defacement; targeted attacks; loss of USB stick; mis-addressed e-mail
- If in doubt, report the incident; whether you feel it might not be important enough or whether you think somebody else has or should have reported it.
- In the event of an incident, the emphasis will be on resolution and learning from lessons.

9. Social Media and Online Participation

- 9.1 DCC recognises the value of social media (SM), particularly as a means of building participation and engagement. However, these tools must be treated with respect and caution as they can introduce risks to DCC's information assets and reputation.
- 9.2 You are personally responsible for any information you publish. Your behaviour online is subject to the requirements of DCC Code of Conduct – as much as it would be in any other scenario.
- 9.3 In line with any other aspect of your work, you must comply with all DCC policies, including those related to information security and data protection.

Use as a DCC employee

- 9.4 If you choose to participate as a council employee you must clearly identify yourself and your role.
- 9.5 Your usage of SM as a DCC employee should be limited to those communities which have been officially sanctioned. If in doubt, seek line-manager approval.
- 9.6 DCC's SM presences are monitored. Any inappropriate use by DCC employees will be investigated and action may be taken under DCC's disciplinary procedures.

Personal use

- 9.7 You must make it clear that the views you express are your own. This is especially necessary if it is apparent from your account profile that you are a DCC employee.
- 9.8 Access to SM while at work is at DCC's discretion and must not affect your performance or productivity at work. Any misuse of this facility can result in it being withdrawn and potential disciplinary action.

Guidelines

- For more guidance on the personal use of SM, consult the Employee Guidance on Personal Use of Social Media.
- For more guidance on the use of SM in a council business sense, consult the Social Media Policy, Procedure and Guidance.
- Although you might think that you've been careful about how much you reveal about your identity, it is possible to combine details from a number of sources to create quite a detailed picture of who you are and where you work.
- Many SM sites incorporate software applications or plugins, some of which can provide a risk to DCC's ICT systems.
- Take care to set your SM privacy settings to limit access to your information and identity.
- Although some SM sites claim to have "secure" or "protected" areas, you need to consider how confident you can be about the level of security and the potential outcome if these security measures fail.

Appendix 1: Email Management Guidelines

1. Clear or delete emails regularly to save on disk space and avoid backlogs which may result in important messages becoming lost or overlooked.
2. Email archives should not be used as overflow storage; these are unsupported by ICT Services and can result in loss of vital records.
3. In-boxes should be kept clear by following the Information Management team's Email Guidance.
4. Set up folders for dealing with your main task areas, or most frequent correspondents. These folders could be controlled by a retention schedule, for example: 1 month, 6 months, one year, six years and permanent.
5. Important information, for example contracts etc. should be extracted from e-mails and stored on a shared area of the DCC network.
6. Attachments should only be used when they are the only efficient method of communicating a document. The preferred alternative is to place the attachment in a shared area and email people with the file name and its location.
7. When you receive an email message with an attachment that needs to be retained, save it to an appropriate networked folder and remove the message and attachment from your mailbox as soon as possible.
8. Sources for information access requests, for example DPA or FOI, include email and therefore regular housekeeping, including the deletion of redundant messages should be common practice. Not doing this increases the burden of disclosure.
9. Subscription to discussion groups or mailing lists should be kept to a minimum; these often generate unmanageable volumes of communications.
10. When going on leave, staff should make use of the 'Out of Office Assistant', giving alternative contact details for urgent messages.

Appendix 2: Safe-Haven Guidelines

Sending information by fax is not an intrinsically secure method. You need to be certain that the information is only handled by specific, authorised people. To ensure this, there need to be very clear procedures in place, including audit trails to demonstrate that the procedures have been followed. The following are high level guidelines. More specific guidance will be available either within your service or from the corporate Information Management team.

- In all cases, think whether it is entirely essential to send by fax. If not, use a more secure alternative. For example, via a *GCSx email* account.
- When we share information with external organisations by fax, we must obtain assurance that these organisations have a designated Safe Haven point for the receipt of *personal information*.
- We must get assurances that they meet the requirements of the Data Protection Act 1998 and Common Law Duty of Confidentiality.
- Safe Havens should be risk assessed before being used. Where the risk assessment demands it, they should be lockable and only accessible to authorised staff. Equipment therein should have a code password and be turned off out of office hours.
- Safe Haven machines must be configured to log all activity. To supplement this, a register should be maintained to identify faxes sent, including: person sending; person receiving; time sent; purpose of fax; acknowledgement received.

When sending to a safe-haven location:

- Be certain that the receiving fax machine has been confirmed as being a safe-haven machine.
- You must be certain that the correct person will receive it and that the fax number is correct (ideally, use a pre-programmed number).
- If you are unsure that the number is correct, test it; send a blank fax to the recipient asking them to confirm receipt and that they are who you expect them to be.
- Use a cover sheet to clearly identify: the Council, service area and section of the originator; the intended recipient; the number of pages sent (including the front sheet) and any reference numbers used. The cover sheet should also explain what a recipient is to do with a misdirected fax.
- Notify the recipient when you are sending the fax and ask them to acknowledge that what they receive is as described on the cover sheet.
- If you need to keep the source paper copy for record-keeping purposes, make sure that you do so securely. Otherwise, ensure that the source copy is securely shredded.

In the event of a problem (e.g. a fax is mis-directed or not received successfully), report it to your line manager as a potential data breach.

Appendix 3: DCC ISMS Document Set

Available corporately

[\[link removed\]](#)

Information Security Policy

A high-level statement of DCC's IS policy framework and related roles and responsibilities. Signed off by DCC Chief Executive.

Personal Information Security Policy

The objective of this policy is to assist in the protection of all information assets, owned and used by DCC, from the risks posed by inappropriate use.

Third Party Access Policy

To ensure that third-parties with access to DCC systems comply with DCC security policies.

Security Incident Management Procedure

To outline the responsibilities for, and actions to be taken, when a security incident is suspected or when notification of such an incident is received...

ICT Asset Control

To ensure that physical ICT assets are registered and managed throughout their lifecycle, in support of Durham County Council's Information Security Management System (ISMS).

Physical Security

DCC's sensitive assets shall be sited so as to ensure that physical security measures are consistent with the nature and requirements of the information and assets being protected.

Available within ICT Services

Business Continuity Plan

To provide a mechanism for ICT Services to restore important systems that meet the needs of the Business Continuity Plan for DCC and its users.

DCC Cloud Hosting Requirements

Requirements for suppliers of ICT solutions to adhere to when tendering for business with DCC. Takes into account a number of factors that are particular to the cloud environment.

Forensic Readiness Procedure

Maximise our ability to collect credible digital evidence; Minimize the cost of forensics in an incident response.

Logical Access Control Policy

To control access to information to authorized personnel only and ensure that access is granted on the basis of business requirements.

Network Security Policy

A consistent approach to the security of DCC networking services by ensuring that DCC information is protected to ensure: Confidentiality; Integrity; Availability.

(continued overleaf)

Appendix 3: DCC ISMS Document Set (continued)

Organisational Arrangements

To ensure that information security is managed effectively and is consistent with organizational objectives.

Systems Development & Maintenance

To ensure that security considerations are addressed as part of the system design and are not compromised during subsequent development or maintenance.

Appendix 4: Metadata and Change History

Title: Personal Information Security Policy

Purpose: To assist in the protection of all information assets, owned and used by DCC, from the risks posed by inappropriate use.

Scope: The scope of this Policy applies to all DCC personnel. Agency workers or sub-contractors who are required to use the ICT systems will also be made aware of, and be expected to abide by, this policy.

Links to other documents: DCC IS Policy

Functional Area: Durham County Council

Version: 3

Author: [removed] **Phone:** [removed] **Email:** [removed]

Owner: [removed] **Phone:** [removed] **Email:** [removed]

Reviewers: IGG; ICT SMT; ICT Security Team

Approval: IGG: Nov 2017

Issue Date: 24/01/2018

Review Frequency: Every three years

Last Review Date: Nov 2017

Next Review Date: Nov 2020

Location: DCC intranet: Information Security page

Document History

Ver	Date	Editor	Notes
1.1	19/08/2011	RD	First draft for review by IS Forum sub-group
2.0	11/09/2012	RD	Final IGG comments
2.1	05/03/2014	RD	Minor updates after comments from IGG & ICT
3.0	14/11/2017	RD	New major version due to significant changes.