



Information Security Document

Information
Safe Haven
Guidance

Version 11.0

Version History			
Version	Date	Detail	Author
1.0	09/10/2007	Completed for distribution to AC and CAYA SMTs	Jo White
1.0	19/11/2007	Approved by Chief Officer's Group	Jo White
2.0	26/06/2009	Approved by Information Governance Group	Don Gibbs
3.0	28/06/2011	Reviewed by Information Governance Group	Jo White
4.0	06/07/2012	Reviewed by Information Governance Group	Jo White
5.0	27/09/2013	Reviewed by Information Governance Group. Confidential replaced by restricted where appropriate. Details of Information Classification & Handling Policy added.	Jo White
6.0	12/01/2015	Reviewed by Information Governance Group. Additions re confidential waste and records management.	Jo White
7.0	07/03/2016	Reviewed by Information Governance Group. Antivirus attack information added. Website links updated.	Jo White
8.0	03/04/2017	Reviewed by Information Governance Group. Confidential Waste procedures updated.	Jo White
9.0	08/05/2018	Reviewed by Information Governance Group. Add GDPR.	Jo White
10.0	10/06/2019	Reviewed by Information Governance Group. Page 4 – IGG chair updated. Page 7 – TNT removed. Pages 9, 10, 18 – Incident reporting updated. References to laptops added.	Jo White
11.0	06/10/2020	Reviewed by Information Governance Group.	Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
A.6.2	Mobile devices and teleworking
A.7.1.2	Terms and conditions of employment
A.7.2.2	Information security awareness, education and training
A.8.2	Information classification
A.8.2.3	Handling of assets
A.8.3.3	Physical media transfer
A.9.1	Secure areas
A.9.3	User responsibilities
A.13.2.1	Information transfer policies and procedures
A.13.2.2	Agreements on information transfer
A.13.2.3	Electronic messaging
A.16.1.2	Reporting information security events

A.18.1	Compliance with legal and contractual requirements
--------	--

Contents Page

INTRODUCTION	5
FURTHER ADVICE	5
WHAT IS AN INFORMATION SAFE HAVEN?	6
WHY DO WE NEED TO CREATE A SAFE HAVEN?	6
HOW DOES THIS APPLY TO STAFF?	6
WHAT PROCEDURES ARE INCLUDED?	6
HARD COPY RECORDS AND SECURITY	7
<i>Disposal of personal data</i>	8
MAIL – INTERNAL AND EXTERNAL	9
Faxes	9
VERBAL COMMUNICATION	12
<i>Telephone Calls</i>	12
<i>Other conversations</i>	13
ELECTRONIC RECORDS	14
<i>Physical security</i>	14
<i>Logical security</i>	14
ELECTRONIC INFORMATION – ADDITIONAL CONCERNS	16
<i>Mobile Computing</i>	16
<i>External Email</i>	16
<i>Incoming Email</i>	17
ESTABLISHMENT SECURITY – VISITOR AND PUBLIC ACCESS	18
TAKING WORK OUTSIDE THE WORKPLACE	19
<i>Taking work home</i>	19
INFORMATION SHARING	20
RECORDS MANAGEMENT AND INFORMATION QUALITY	20
MANAGEMENT OF RESTRICTED INFORMATION FLOWS	21
POTENTIAL BREACHES OF SECURITY OR CONFIDENTIALITY	21
AVOIDING VIRUS ATTACKS	22
APPENDIX I - RESTRICTED INFORMATION FLOWS AND CONTROLS	23
APPENDIX II - TAKING WORK HOME	24
APPENDIX III - CHECKLIST - INFORMATION SAFE HAVEN PROCEDURES	26
APPENDIX IV - COMMON LAW DUTY OF CONFIDENTIALITY	27
APPENDIX V – HUMAN RIGHTS ACT – <i>Article 8</i>	28

Introduction

There are many well publicised stories about large organisations that fail to protect personal data properly by not implementing a few basic procedures. There are also examples of organisations that, by not sharing the information that they hold, fail to protect individuals.

This guidance is intended to help increase understanding and improve the control of restricted and controlled information as it moves into, around and out of the Council. These procedures build on the guidance that already exists, e.g. <https://staff.derbyshire.gov.uk/information-security/information-security.aspx> and are designed to ensure that measures are taken to protect information and that information is appropriately and properly delivered so that any necessary action may be taken.

This document details procedures to keep business sensitive and personal data private and secure, but accessible when required. It is one of the key documents in the Council's Information Governance Framework, the standard for managing confidentiality and access to information in the Council.

This document aims to provide a consistent approach and guidance on the correct way to handle personal data and to help ensure consistency

This guidance applies to all employees of Derbyshire County Council, elected members, partner agencies, contractors and vendors. This guidance is subject to annual review by the Information Governance Group and periodic compliance checks by Audit Services and the ICT Service.

Further advice

For further clarification with regard to this document or any other Information Governance document, check the guidance available on the Council's website or contact your departmental representative on the Corporate Information Governance Group, chaired by the Director of Finance and ICT.

What is an Information Safe Haven?

An Information Safe Haven is the objective behind the set of procedures that ensure the safety and secure physical and electronic handling of personal data whilst the information is located within Derbyshire County Council and covering flows of such information within it and to other agencies.

Why do we need to create a Safe Haven?

Safe Haven procedures must be in place in any location where data is being received, held or communicated. All parties must comply with the Information Safe Haven procedures to ensure that the privacy and confidentiality of information is maintained where appropriate and to comply with legal obligations placed on the handling of such information under the Data Protection Act 2018, the Common Law Duty of Confidentiality (Appendix IV) and the Human Rights Act 1998 (Appendix V).

How does this apply to staff?

All staff must be aware of their responsibilities for secure personal and restricted information handling and comply with the Subject Access Request Procedure, Information Security Management System and the Data Protection Policy. However, it is the responsibility of managers, senior managers and strategic directors, for all staff reporting to them to have received appropriate training in information security and confidentiality.

To quickly assess compliance with this guidance there is a checklist in Appendix III.

What procedures are included?

To create an Information Safe Haven the following areas need to be addressed

- Hard copy record security;
- Mail internal and external;
- Verbal communication;
- Electronic records;
- Establishment security;
- Taking work outside the workplace;
- Information sharing;
- Management of restricted information flows;
- Potential breaches of security or confidentiality.

Hard Copy record security

The Council's Information Classification & Handling Policy and Information Classification & Handling Procedures describe in detail how information and data should be classified, labelled and handled. staff.derbyshire.gov.uk/document-classification

This section is concerned with restricted paper records when they are in use and when they are not.

- Do not leave restricted or personal information on display when leaving a desk for a period of time, take basic precautions and put it away. For longer absences it should be locked away or returned to filing cabinets. This will help to prevent disclosure through the casual scanning of documents.
- Store personal data and other restricted information in locked filing cabinets, returning them to these filing cabinets whenever possible. If files have to be left somewhere because they are being worked on make sure that they cannot be easily viewed by anyone else. Lock them in a desk or office if possible when they are not in use.
- Avoid locating faxes, photocopiers and printers in public areas. If printers are being shared, are others able to read restricted information or retrieve it? Wherever such devices are located pick up such information from the printer or fax promptly. Do not leave it where other people may take it or read it accidentally.
- Spoiled photocopies and prints may still be restricted. Do not put them straight into the wastepaper bin: dispose of them as confidential waste. If a photocopier is jammed or a printer halted with restricted information still being processed, take steps to retrieve this information as soon as possible to prevent disclosure.
- Lock your prints that are sent to multifunction devices (MFDs).
- Take care in selecting the correct recipients when using the email function of printers (MFDs) to send copies of scanned documents.
- Always check that originals have been removed from the photocopier as well as copies. This is one of the most common ways of losing and disclosing restricted information.
- Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.

- Keep clear desks as this is an obvious way of preventing any confidentiality problems arising from having visitors at desks, or disclosure when desks are left unattended. A clear desk will help to protect against the disclosure of information.
- Hard copy files (including other types of media) and boxes which are due for storage (or disposal) e.g. to be collected by authorised third party companies, must be kept securely until collected.

Disposal of personal data

Not adhering to corporate guidance about the disposal of restricted information can lead to disclosure, which is a breach of the Council's obligations under the Data Protection Act 2018 and may lead to disciplinary action and potentially large fines being issued by the ICO. Disclosure can most easily happen when getting rid of surplus notes, photocopies and printed copies that are made every day. Any papers that are going to be disposed of should be checked for personal data.

See also Corporate Record Disposal and Confidential Waste procedures staff.derbyshire.gov.uk/disposing

There are two options for dealing with this: shredding it (where available) or putting it in a confidential waste bin (if you are not sure, speak to your Business Services Manager about appropriate disposal facilities). All confidential waste must be disposed of properly using Council provided, lockable waste bins wherever they are available. Alternatively, sites not on the Matlock complex needing to use a confidential waste provider should use the Council's confidential waste contract with Shred Station. Do not dispose of confidential waste in wastepaper bins, office bins, kitchen bins or anywhere else other than approved waste disposal bins.

Destroying information earlier than necessary may be a breach of the law so it is important that departmental retention periods are checked before destroying any records. Retention schedules can be found at: staff.derbyshire.gov.uk/retention-schedules

Mail – internal and external

Restricted mail sent by internal or external post is not always marked as such or correctly addressed and because of this there is a need to have secure mail handling procedures in place. For internal mail there is sometimes a more relaxed attitude to dispatching information, for example, not using envelopes. For restricted information this is inappropriate and should not occur as it can lead to disclosure.

All mail is delivered, opened and sorted at the Derbyshire Business Centre (DBC) by appropriately trained staff in a secure environment. The DBC is expected to comply with the guidance detailed below where appropriate but there is still a need for Departmental procedures for dealing with internal and external mail. These procedures should include:

- A single point of mail delivery and handling that is subject to standard procedures and ensures that there is always someone available to deal with incoming and outgoing mail for each team. Post should be opened and dealt with away from public areas.
- Staff must ensure that any mail marked: Private, Confidential or Personal, or any combination of those or similar terms, is only passed to the named recipient unless a prior delegation arrangement has been made. It is appropriate to have these arrangements set up so that no restricted post remains unopened e.g. because the recipient is off work. Private personal mail should not be sent to work addresses.
- Any restricted post that is not immediately given to the recipient must be kept safe until they can receive it. The member of staff in possession of the information is responsible for it until it is handed over.
- Post trays and 'pigeonholes' should be securely located, but unsealed, restricted documents should not be left in them.
- Treat any documents that arrive containing personal or restricted information, but not necessarily marked as such, as above.
- All sensitive records must be stored face down in public areas and should not be left unsupervised.
- If outgoing post contains restricted information the envelope should be marked as 'Private and confidential' and 'to be opened by addressee only'.
- Restricted documents should only be sent to a named person.

- Consider whether the use of special delivery or personal delivery might be appropriate to the circumstances and nature of the restricted information being sent. Further information and guidance is available in the Information Classification & Handling Policy and Information Classification & Handling Procedures staff.derbyshire.gov.uk/document-classification
- Where internal mail is being used to send restricted information, the documents must be in envelopes marked 'confidential'. Do not send forms, memos or minutes with personal data on them through the internal mail without being sealed in envelopes. This also applies to personal data for and about staff.
- When internal mail is being transported between Council sites it must be protected from damage or loss. If this transit includes personal data, the process should be recorded under an information sharing agreement.
- Make sure that the establishment post box is clearly visible to visitors wanting to deliver post by hand.
- If post goes astray or is issued to the incorrect address notify your line manager immediately and if the information contains restricted or personal data, this must be reported as an information security incident in accordance with the Council's Security Incident Management Policy and Procedures staff.derbyshire.gov.uk/report-security-incident

Faxes

A fax machine allows restricted information to be transmitted electronically between locations so needs supporting security procedures to ensure secure delivery. Faxes are not seen as a safe way of transmitting information and should be used as a last resort. Secure, encrypted email should be used in place of faxes wherever possible in accordance with the Council's Secure Email Policy: staff.derbyshire.gov.uk/sharing-info

Receiving faxes:

- Locate fax machines in a secure area where casual passers-by and visitors cannot see the faxes.
- Assign staff to receive incoming faxes and ensure they reach their intended recipient promptly. They should not be left lying by the fax

machine or risk falling behind or underneath and so being unseen. If the fax is not collected the same day, it should be placed in a sealed envelope marked 'confidential' and sent to the intended recipient.

- Ensure the fax has paper in it otherwise receipt of faxes may be delayed at inappropriate times.
- Occasionally, restricted faxes will be received where the intended recipient is not clear. In these cases, they should be passed to a nominated person within that location.

Sending faxes:

- Only send restricted information by fax when absolutely necessary. Check with the recipient that their fax machine is securely located, warn them to expect a restricted fax and ask them to confirm when they receive it.
- When sending faxes, check to make absolutely sure that the fax-number being sent to is correct. Commonly used numbers can be programmed into the fax machine to avoid misdialling.
- If there is uncertainty that the fax went to the correct number, check it on the machine. If this confirms the information went astray, report it to line management straight away. If the information contains restricted or personal data, this must be reported in accordance with the Security Incident Management Policy and Procedures: staff.derbyshire.gov.uk/report-security-incident
- Use a fax coversheet that contains a confidentiality statement e.g.

“This fax is restricted and is intended only for the person/s to whom it is addressed. If you have received this fax in error, please immediately notify us by telephone on the number above and return the message to us by post. If the reader of this fax is not the intended recipient, you are hereby notified that any distribution or copying of the message is strictly prohibited”.

The Council has a programme of replacing fax machines wherever possible with MFDs - where the print should be locked and released by the individual using their own PIN. This is a far more secure method.

Verbal Communication

Telephone Calls

When a telephone call is received, staff often have little control about where they might be, particularly with mobile phones, so sometimes when answering the call, personal data could inadvertently be disclosed to people listening nearby. The same issues arise when talking to service users or colleagues.

Secure and confidential practice would include: -

- Not making or receiving telephone calls which can clearly be overheard e.g., in reception or public areas. If such a call is received, go to a more private area and call the person back. Consider whether it is appropriate to continue the phone call in your office if there are other employees present even if they are from the same team.
- Ensure that you are talking to the correct person that is authorised to deal with the transaction/work by verifying their details. Internally, do not assume that the name on the phone is the person you are speaking to. In the case of an organisation, it may be appropriate to call them back to verify their credentials.
- If it becomes necessary to leave the phone for any reason, put the caller on hold so that they cannot hear other potentially confidential conversations that may be going on in the office.
- If a message needs to be taken and left on someone's desk, ensure that these messages do not themselves contain restricted information.
- Do not leave confidential or sensitive messages on an answer machine as these can be reviewed by people other than the intended party.
- Requests for information under the Data Protection Act 2018 and the Freedom of Information Act 2000 should be made in writing. The caller should be asked to make their request in writing either by email to access2info@derbyshire.gov.uk or by letter to Access to Information, Commissioning, Communities and Policy, County Hall, Matlock, Derbyshire. DE4 3AG.

Other conversations

Similar considerations apply as for telephone calls. Staff should remember that even though they may be on Council premises there may be other people from other organisations or teams present.

- When having a meeting or interview with someone where restricted information will be discussed, ensure that there is sufficient privacy, for example in a meeting or interview room. Check that the room is suitable.
- Even in the office environment, restricted information should only be discussed with colleagues who need to know the information in order to carry out their job.
- Always consider your surroundings and the proximity of others who may be able to hear in non-Council establishments e.g. public houses
- Always record who is present at meetings where restricted information will be disclosed. If an external agency is present an information sharing agreement should be in place.

Electronic Records

IT devices present a range of different security issues, the main issues are highlighted below. For job roles that require staff to know more, there is further guidance available at <https://staff.derbyshire.gov.uk/information-security/information-security.aspx> and also from the ICT Service Desk.

For the purposes of the Information Safe Haven Guidance controls for ICT can be divided into two broad areas:

Physical security

- Ensure that PCs, laptops and screens are sited away from public areas so that unauthorised people cannot read the screens e.g. through windows or while waiting in public areas.
- Take the same care with the location of printers, especially shared printers (see above).
- If restricted information has to be transferred to portable media, such as disks, CD, memory cards, etc, ensure that these are securely managed and that the information is not left on this media indefinitely. The safest location for all restricted information is on the Council network. Where it is necessary to transfer data to portable media the media must be encrypted with appropriate security software. Data should not be stored on local hard drives.
- PCs, laptops or any other computing devices should not be left in areas accessed by the public (see Mobile Computing below).

Logical security

These are security measures implemented via a PC, laptop and network software to prevent unauthorised disclosure of information or the misuse of the PC. They are mainly based around network or application (e.g. SAP) access control and the information access rights granted to individual users.

- Password control. Do not share passwords with anyone, and do not use anyone else's password. It can be a disciplinary offence to use another person's password or knowingly let someone use your password. You are responsible for all transactions undertaken on the County Council's network which are assigned to your network id.

- Do not write passwords down. If a member of staff suspects that their password is no longer secret then they must change it immediately.
- Make passwords hard for anyone else to guess by incorporating numbers, special characters and mixed case into it. Some systems will force this already. See the Council's Password Policy for rules around length of passwords and using passphrases.
- Lock PCs and laptops using **Ctrl-Alt-Del** or the **windows key and 'L'** whenever leaving screens unattended. This will prevent anyone accessing any restricted information on the PC or laptop while it is unattended.
- Do not store any information on local disk drives as this is not secure and is subject to loss as it is not backed up onto the corporate network. Always save information on the network. Information on the network is better protected against data loss than data stored in other locations including the hard drive.
- The access rights that are allocated to staff on the network are designed to give them sufficient access to the information that they need to do their job. Staff should make themselves aware of who else can access restricted information when saving on any particular network directory. The principle, as with paper records, is that it should only be available to those who need to see it. This is likely to be supervisors and perhaps certain other members of the team. If unsure who can access it, staff should check with their line manager. If you have access to information that you do not require to fulfil your current role, you should notify your line manager immediately.

All staff should make themselves familiar with the Council's rules for the use of Internet and Email as laid out in staff.derbyshire.gov.uk/internet-email

Electronic information - additional concerns

Mobile Computing

There are additional risks associated with the use of any mobile device capable of storing or communicating information, which go further than just being the electronic equivalent of transporting files. There is the potential for the loss of the device through misplacement or theft. Any mobile device that holds restricted information must have data encryption to make any information on the device unreadable. All Council mobile devices should be adequately secured in a vehicle's boot whilst being transported. Mobile devices should not be left in vehicles unattended. There is also an issue of whether the wireless communication (if used) is securely configured. These issues will normally have been addressed by the ICT Service before equipment is issued, but any queries should be referred to line management. For further information see Desktop and Mobile Device Security Procedures. staff.derbyshire.gov.uk/mobile-working

External mail

There is an increasing expectation for staff to use email to communicate externally (i.e. to non 'derbyshire.gov.uk' addresses) with service users and external agencies via the internet as this gives instant and apparently guaranteed delivery. However, email is not a secure route for sending restricted information.

One of the main reasons for this is that email copies reside on all servers through which they are transmitted, and each transmission can go through several servers/countries which may be vulnerable to hacking. Hacking is becoming more common, especially as incidences of identity theft are increasing; personal data is exactly what identity thieves require. Staff should be aware that there is an increasing threat of organised crime looking for such personal data to commit identity theft. Hence, especially given the sensitive nature of the personal data the Council handles, it is current policy not to send personal data by unencrypted external email.

- Do not use any other email service than that provided by Derbyshire County Council to send restricted information by external email. Personal data should only be sent externally via the encrypted email service or other government networks facilitated by the Council.
- The Council will provide a process by which service requests may be made to the Service Desk for data which needs to be encrypted to ensure the security and integrity of data which needs

to be emailed to other Council locations, external organisations and partner agencies. Encryption levels of data on such documents must be a minimum of 128bit AES - in line with the Council's Encryption Policy. Sensitive and person identifiable information and data must not be emailed unencrypted.

- Records of personal data sent by email (internal or external) are accessible to the data subject if they request access under the Data Protection Act 2018.
- Do not forward Council restricted email to accounts for private use.

In the same way that post needs to be dealt with promptly, so does email. A colleague/manager should be assigned to check staff email inboxes when they are off work so that urgent or confidential matters can be dealt with and any delegated permissions should be periodically reviewed to ensure they remain accurate.

For further information on rules, good practice and the use of email and the internet see: staff.derbyshire.gov.uk/internet-email

Incoming Email

Although the Council does not have total control over the emails received, employees must be aware of the dangers of opening messages from unknown or not trusted sources.

Email attachments or links from unknown senders should not be opened. If the email attachments or links are from senders you do know but you were not expecting the email as part of council business e.g. invoices for payment, you should not open them and should report them as a security incident.

If the intended recipient is not the actual recipient, the sender should be informed that the message has not reached its intended destination and has been deleted.

Establishment Security – visitor and public access

With many different offices and work locations across the Council, it is important that the Council seeks to maintain to a basic standard of physical security at all locations where personal data is held. Maintaining the security of office areas and ensuring that wherever possible they are separated from the public areas is an important element in this. The basic steps below are good practice and will help to protect staff and property as well as confidentiality.

- Make sure that all visitors sign in and out at all times and disclose who they are coming to see.
- Visitors should be supervised at all times.
- Staff should be encouraged to challenge anyone in office areas if they do not know who they are, e.g. if they are not accompanied by a member of staff or they are not wearing a Corporate ID badge.
- Staff should be aware of anyone they do not know attempting to follow them through a security door and if appropriate be prepared to escort them back to reception or the public area if necessary.
- Managers should ensure that all paper-based records and any records held on computers are adequately protected by establishment security. Risk assessments should identify any potential threats and an appropriate risk management strategy should be produced
- All staff must wear their Corporate ID badge on Council premises and report losses or thefts immediately to their line managers. All such events must be reported in accordance with the Security Incident Management Policy and Procedures: staff.derbyshire.gov.uk/report-security-incident

Staff in residential establishments will need to check their local procedures whilst working inside the home.

- Members of the public who do not want to discuss their private matters with a receptionist in a public area should be offered the opportunity to be seen elsewhere.

Further information is available in the Access Control and Premises Access Control Policies: staff.derbyshire.gov.uk/access-buildings

Taking work outside the workplace

Wherever staff are working on, or in possession of, work-related data e.g. in the office, on the phone, at home, en-route to or from the office or home, at meetings, conferences, court hearings and so on, they are responsible for it. If information is handed out at court, in conferences or meetings, the same person is responsible for collecting it back in at the end or ensuring it is only in the hands of those authorised to keep it. Line Managers should have procedures in place to record the location of the County Council's Information outside of the workplace.

Taking work home

As the Council increasingly uses electronic records, paper records will inevitably be used less, however, the guidance provided on securing paper files still applies. Staff are responsible for safeguarding mobile & electronic records, equipment and electronic storage devices containing, or giving access to, work-related records, just as they are responsible for safeguarding paper records.

Failure to safeguard information or improperly disclosing it may result in disciplinary action being taken against employees and in certain circumstances, may amount to a criminal offence.

The proper place for work-related information is in the workplace. This is where others who need it expect to find it. The proper place for work-related personal data is in locked cabinets (or similarly secure storage) in the workplace. Work-related information must not be kept at home, except by staff whose workplace is their home (See "*Homeworking – A Guide*", issued by Human Resources, which explains the required security arrangements for home-based staff).

<https://staff.derbyshire.gov.uk/your-wellbeing/work-life-balance/homeworking/homeworking.aspx>

If there is a need to take records or files home to work on, appropriate safeguards must be applied to keep them safe and secure.

Appendix II gives more detailed guidance on the measures that should be taken to protect information taken away from the office.

Information sharing

Where restricted or personal data is being regularly shared with other agencies then arrangements must be made for that information sharing to be done in a controlled way that meets ethical and legal obligations. This is done under an information sharing agreement that sets out how the sharing will operate and the standards of management that all parties to the agreement must comply with.

Information on sharing and handling information is available here: staff.derbyshire.gov.uk/sharing-info

There are currently 3 sets of guidance

1. Information sharing protocol
2. Information sharing agreement: template
3. Information sharing framework

All staff involved in such inter agency data sharing must be aware of the details of any existing information sharing agreement and the obligations that it places on them.

Such an agreement will define exactly what information will be shared and how, including the method, transmission or communication between agencies or any shared access security arrangements. The aim is to ensure that Information Safe Haven arrangements operate in the participant agencies and ensure the continued confidentiality of shared information. If staff are unclear on what basis information is being shared with another agency, whether an information agreement exists and what obligations that might place on them, it should be clarified with their manager.

The arbiter of a requirement to access restricted information will be the Access to Information Officer.

Records management and information quality

Confidentiality and security controls for information are undermined if the information that is being protected is for example inaccurate, out-of-date, or misfiled. Procedures to prevent this are outside the scope of this document, but both manual and electronic records should be subject to controls and checks to ensure that the quality of information is assured and the records are managed to current best practice standards.

Under Section 46 of the Freedom of Information Act 2000, local authorities are required to comply with the Lord Chancellor's Code of Practice on Records Management, see:

<https://staff.derbyshire.gov.uk/information-security/information-governance/records-management/records-management.aspx>

for a link to the Council's Corporate Records Management Policy and associated procedures concerning this, which staff must comply with.

Management of restricted information flows

It is important that all managers are aware of all flows of restricted information to and from their area of service, so that they can ensure that the appropriate protection and procedures are applied. In this respect it is important to know:

- What the different sources of restricted information are.
- What communication method is used to deliver the information.
- Where it is received.
- What data protection procedures are in place at each arrival point to protect it and how restricted information is subsequently processed and managed.
- What actions should be triggered and how to ensure that these happen.
- How restricted information is communicated to other agencies or partners in a controlled way. For example, where information sharing with other agencies is necessary on a regular basis there should be an information sharing agreement in place.

Appendix I summarises some of the information flow issues and the possible controls.

Potential breaches of security or confidentiality

If staff become aware of security or confidentiality problems at any location arising from work practices or local procedures they must report these to a supervisor or manager immediately and if it is thought that a breach has occurred this should be reported via the Council's Security Incident Management Procedures. staff.derbyshire.gov.uk/report-security-incident

Avoiding Virus Attacks

There are lots of harmful computer viruses appearing every day that could make their way onto your PC, laptop or other devices if you don't keep them safe. This could not only cause you to lose everything on your device but could have a devastating effect on the Council's network and data records.

You can help avoid virus attacks by:

- Not opening any email attachments or links from unknown senders.
- Not opening any email attachments or links from senders you do know if you were not expecting the email as part of council business e.g. invoices for payment.
- Only using Derbyshire County Council provided encrypted USB sticks – you can request these from the Service Desk.
- Not trying to download software from the internet or from anywhere else.
- Regularly connecting your laptop, mobile or tablet to the network to keep the antivirus software on them up-to-date. This needs to be at least 90 minutes to allow the software to update.
- Not using unsupported versions of word and excel ie .doc or .xls. You should change old versions as you come across them by opening them and then saving as 'word document' or 'excel workbook'. Clicking save will keep them in their 'old' format.
- Not attempting to access your personal webmail using council devices.

If you think that your PC, laptop or any other device has a virus:

- **take note of any messages displayed on the screen**
- **turn the device off with the power button (do not shut down)**
- **call the Service Desk immediately on 01629 5(37777).**

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.

Appendix I - Restricted Information Flows and Controls

Incoming				Outgoing			
Source	Media	Destination	Safe Haven Controls	Source	Media	Destination	Delivery Controls
<ul style="list-style-type: none"> Public or Service Users Other Agencies Other Directorates or Departments Colleagues 	<ul style="list-style-type: none"> Facsimile Royal Mail or Courier Telephone call & case recording Visit from non DCC person Telephone message Internal mail Hand delivery by colleague Discussion or interview & case recording File transfer Email via Internet Email via DCC network SMS text message Shared ICT 	<ul style="list-style-type: none"> Facsimile Postal delivery address Internal Mail Desk Phone Establishment Reception Letter Box Desk Pigeonhole Desk PC via Outlook Desk PC via Internet Desk PC via Business Application (e.g. Mosaic) Mobile device Employee home 	<ul style="list-style-type: none"> Location security: Visitor security and staff ID Hardcopy security: Restricted disposal, filing & clear desk etc. Mail procedures Fax, printer and photocopier location Verbal communication ICT Physical Controls: PC location ICT Logical Controls: User IDs & passwords Computing at home Records kept at Home: Record logs, security arrangements Information Sharing Agreement 	<ul style="list-style-type: none"> Employee / Temp /agency worker Contractor Consultant Partner agency staff From locations: Office Home Service user's home or other location 	<ul style="list-style-type: none"> Fax Telephone PC / Notes /DCC network PC / DCC Network/ Internet Shared ICT PC / DCC Network/ Business application Royal Mail Courier Delivery by hand Internal mail Verbal by discussion or interview Wireless device File transfer 	<ul style="list-style-type: none"> Public or service users Other agencies Other Directorates or Departments Colleagues 	<ul style="list-style-type: none"> Confirmation of receipt Secure e-mail (DCC) Insecure Email (Internet) Encryption Internal mail procedures Postal delivery options Checking receipt of faxes Interface controls Checking delivery addresses Care of manual records in transport Record logs of files transferred Record of details passed on by phone or at meeting Information Sharing Agreement

Appendix II Taking Work Home

The following guidance gives some practical rules on handling people's personal data sensitively, professionally and ethically and to comply with the law:

Staff:

- Must be fully aware of and accept the terms and conditions for taking work home before being allowed to do so. Staff are personally responsible for the security of personal data they hold in connection with their work for Derbyshire County Council.
- Must comply with their team's system to log which records are being taken from the workplace and when (see below). Staff should normally only take home what can be finished and returned to the office the next working day. Any exceptions to this must be agreed beforehand with line management.
- Should something prevent the returning of the records the following day, staff must inform their manager who will ensure the delay is logged. This will save time, should they be needed for other purposes.
- If records are returned late on a regular basis, management will need to address this with the staff member concerned.
- Must remove records from, and return records to, their proper location, within a secure container. Loose bundles of paper, open-top carriers and plastic bags are not acceptable. It is strongly advised to transport records in lockable briefcases.
- At any time that work-related records are away from their normal location, the staff member is responsible for their security. Leaving them unattended for any reason isn't secure e.g. leaving them in the boot of a car, even if the car is in the garage overnight. If taken on work-related visits, they must be kept secure.
- Unless the official workplace is the home, Service User records must not be set up at home whether on PC or in paper form. Official home workers must only set up systems or records at home that has been authorised. All information about service users must go only on the official record or file.
- Remember that paper records at home are inaccessible to staff who may need the information.
- At home, all personal data must be safeguarded from access, no matter how unintentional, by anyone who has no need to know such as family and friends. This would be an unauthorised disclosure.
- Lock papers away securely from general living areas, open doors and windows in the same way that personal valuables would be looked after.
- Passwords protect PCs.
- Remove storage devices from the PC, and printed copies from the printer.
- See separate guidance on emailing personal data and faxing personal data.
- Virus control is vital. Do not mix home and work storage devices. All storage devices used to transfer information to and from home must be virus-checked each time they are returned to the workplace.
- To comply with the Copyright Act, all software used to process service user records must be legally purchased.

- Report any breach of security or confidentiality immediately to line management and via the Council's Security Incident Management Procedures.
- This includes loss or theft of work-related information. If a crime is involved, report it to the police immediately.
- Bring all paper waste containing work-related personal data to the office for restricted disposal. Never dispose of it via household waste or recycling bins.

Managers:

- Managers are responsible for the security of personal data held by members of their team(s) in connection with their work for the Council. This guidance will help to fulfil that responsibility.
- It must be agreed in advance with the staff concerned: what/how many records they can take home, when and for how long if planned to be for longer than to the next working day. This will vary, depending on the nature of the team, but two balancing considerations will help decide:
 - Staff should normally only take home what they can finish and return to the office the next working day.
 - Staff care includes achieving an appropriate work-life balance. Taking work home should be exceptional, not frequent or too regular.
- Managers must authorise and log any exceptions to this.

Managers must ensure a log is kept of which records staff are taking from the workplace and when. (Appendix II gives further details.) Managers should assign staff to maintain and routinely check the log and to alert them to any records that are not returned on time. Should something prevent staff returning the records on time, they need to explain the delay to their manager. Ensure this is also logged. This will save time, should someone else need the records for other purposes.

- If staff members return records late on a regular basis, this will need to be addressed with them. Late returns must be the exception.
- Staff must only set up any systems or records at home that have been authorised. Normally, this means none: the exception being staff whose workplace is their home. They must only use authorised systems. All information about service users should go only on the official record or file.

A log of records removed from the workplace should record the following:

- Record: PIN; family name; record type (hard copy, electronic copy); date removed; by whom; date to be returned; reason for extended timescale; authorising line manager; reason if not returned by due date; date returned.
- For paper records, put a card/sheet in place when the file is removed from its place in the filing cabinet (or its expected, secure storage).
- Keep a chronological log of the same information (can be paper, word document, spreadsheet to suit the team/section).

Appendix III Checklist - Information Safe Haven Procedures

Ref	Question	Never	Sometimes	Always
1	Where you work do visitors always have to sign in?			
2	Are visitors always supervised in office areas?			
3	Do visitors have privacy when explaining confidential matters to the receptionist?			
4	Do you wear your ID badge?			
5	Would you challenge someone you did not know in the office area?			
6	Do you keep a clear desk?			
7	Do you return records to the filing system when you are not using them?			
8	Do you lock restricted records away when you are away from your desk?			
9	Where you work are faxes, printers or photocopiers sited in public areas?			
10	Do you use a shredder to dispose of unwanted confidential notes?			
11	Do you use the confidential waste bins?			
12	Do you check papers before you recycle them for personal data?			
13	Do you know how long you have to keep the records that you deal with?			
14	Do you envelope any personal data sent through the internal mail?			
15	Do you mark envelope contents as restricted and send it to a named person?			
16	Do you check confidentiality arrangements with the recipient before sending restricted faxes?			
17	Do you send faxes, emails and letters with a covering confidentiality statement where necessary?			
18	Do you leave records in your car?			
19	If you work at home do you have security arrangements in place to prevent disclosure of records to relatives and friends?			
20	Do you check whether you can be overheard by anyone who should not hear before discussing confidential information?			
21	Do you check a person's identity and their right to information before disclosing confidential information?			
22	Do you keep your password and your user id confidential?			
23	Is your PC sited so that no unauthorised person can see information on your screen?			
24	Do you only store electronic records on the DCC network?			
25	Do you lock your PC screen when you leave your desk?			
26	Do you send personal data by external email?			
27	Do you use your private email address for work purposes?			
28	Have you delegated someone to check your emails and post when you are off work?			
29	Do you know the terms of any information sharing?			
30	Do you know how to record a security incident?			
31	Do you know where to get further advice if you need it?			
32	Is your computer switched on at least every 30 days to keep it up to date with antivirus and patches?			

Appendix IV

The Common law Duty of Confidentiality

Where an individual has not given their consent to the use or disclosure of information for a purpose, which is different to that which was originally intended, it will need to be carefully considered whether a duty of confidence exists.

The law imposes a duty of confidence whenever a person requires information which he knows or ought to know is fairly and reasonably to be regarded as confidential. (Campbell v MGN Ltd [2004] UKHL 22)

In order for an action for breach of confidence to be brought, the following 3 criteria need to be satisfied:

- **The information has a quality of confidence:**
It must not be something that is public property or public knowledge
- **The information became known in circumstances imposing an obligation of confidence (legitimate expectation):**
This obligation may be imposed by contract or be implied by the relationship between the parties involved i.e. employee / employer. Whether the obligation exists is a matter of reasonableness namely whether a reasonable man, standing in the shoes of the recipient of the information, would have realised that upon reasonable grounds, the information was being given to him in confidence
- **There must be an actual or threatened unauthorised use of that confidential information to the detriment of the party communicating it:**
Information may have been disclosed for a specific, limited purpose and so any use of the information beyond this purpose would be a breach of confidentiality. For example, information disclosed for the purpose of confidential negotiations could not later be used against the imparting party, for a different purpose as to do so would be a breach of confidence.

(Coco v AN Clark (Engineers) Ltd [1969] RPC 41)

Appendix V

The Human Rights Act 1998

Article 8 of the European Convention on Human Rights– Right to respect for private and family life

Article 8(1) provides that everyone has the right to respect for his private and family life, his home and his correspondence.

In order for a public authority to justify any interference with the exercise of this right, it must satisfy the criteria in Article 8(2), namely that any interference must be;

a) **In accordance with the law;**

In order for an interference to be in accordance with law, the interference must have a proper legal basis, such as a piece of legislation or rules of a professional body. The law or rule must be understandable, detailed and clear enough to allow a person to regulate his or her behaviour - a secret, unpublished memo in a government department will not suffice, for example.

b) **In the interests of ‘The Legitimate Objectives’;** and

These are set out in Article 8(2) as being any interference which is;

- in the interests of national security, public safety or the economic well-being of the country;
- for the prevention of disorder or crime
- for the protection of health or morals
- for the protection of the rights and freedoms of others.

c) **Necessary in a Democratic Society**

Even if the infringement of privacy is in accordance with the law, and it is for one of the legitimate objectives, it must still be ‘necessary’ in order for it to be justified under Article 8. This is the third and most stringent condition that any infringement must satisfy, bringing in a requirement that the act must be ‘proportionate’.