Information handling / safe haven procedure

Version: 4
Date Issue: November 2018
Review date: November 2019
Reference: WCCC-1073-347
Team: Information Management
Protective Marking: Public

Warwickshire
County Council

Contents

Changes and approvals

V1	Information Governance Steering Group	January 2015
V2	Information Governance Steering Group	17 January 2017
V3	Information Governance Steering Group	27 March 2018
V3.1	Information Manager & Data Protection Officer (revised for removal of GCSX email)	23 October 2018
V4	Information Governance Steering Group (revised to replace 3.5,3.6; add 2.3, 3.7)	20 November 2018

Author: Information Manager and Data Protection Officer

Contact:

Information Management, Resources Directorate, Warwickshire County Council

Internal - informationmanagement@warwickshire.gov.uk

External: dataprotectionofficer@warwickshire.gov.uk

1. Introduction

The Information Safe Haven and Handling procedure is intended to provide a consistent approach and help on the correct way to handle internal, personal and confidential information as it moves into, around and out of the Warwickshire County Council (WCC).

These procedures are **mandatory** and **must be followed by all staff** as part of the council's Information Governance Framework the standard for managing information in the council and is one of the linked procedures in the Information Compliance policy aimed at all staff

The WCC Information Risk and Protective Markings standard describes how information should be classified according to risk and marked to protect the information when handling. The use of the word 'confidential' here refers to information classed as both Confidential and Confidential-Restricted, including all types of personal information, unless otherwise stated.

This procedure is subject to regular review by the Information Management service to improve handling from user feedback, learning from incidents and application of new technology.

What is an information safe haven?

Safe Haven is a standard term in use throughout health and social care, the NHS and its partners. It is a standard laid down by the Health and Social Care Information Centre as part of their duty under the Health and Social Care Act.

An Information Safe Haven is the outcome of a set of procedures that ensure the safety and secure physical and electronic handling of personal data whilst the information is located within the council and covers flows of such information within it and to other external partner agencies.

Why do we need to create a procedure?

The Information Handling and Safe Haven procedure to ensure that the privacy and confidentiality of information is maintained when appropriate and to comply with legal restrictions placed on the handling of such information under the Data Protection Act General Data Protection Regulation, the Common Law Duty of Confidentiality and the Human Rights Act.

Flexible working and mobile technology create additional hazards for protecting information as we work outside the traditional protected office boundary. We still transport paper documents everyday between offices, to customers and partners and these require the same level of security.

Don’t forget that we are still responsible for customer information, even if it is being handled or processed outside the council because the service has been commissioned. These standards and procedures also represent best practice in managing information and apply across all services in the council.

How does this apply to staff?

All staff must be aware of their responsibilities for handling all types of information. These procedures apply to all staff of Warwickshire County Council; employees, elected members, partner agencies, contractors and suppliers working for WCC. Failure to comply could result in disciplinary or contractual action against the individual.

There is a checklist at Appendix A that can be used to test your understanding.

How does this apply to managers?

It is the responsibility of managers and directors at all levels, to make sure all staff reporting to them to have received appropriate training in information compliance and promoting understanding of these corporate procedures and any local procedure within their teams.

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

- what the different sources of confidential information are;
- what communication method is used to deliver the information;
- where it is received;
- what data protection procedures are in place for personal information at each arrival point to protect it and how it is subsequently processed and managed;
- what actions should be triggered and how to ensure that these happen;
- how confidential information is communicated to other agencies or partners in a controlled way.

Further advice

If you need clarification on a specific topic, please look on the Information Management i.warwickshire pages, contact Information Management or the ICT Service Desk.

www.warwickshire.gov.uk/im

Information Management , Resources Directorate, Warwickshire County Council

2. Creating, storing and managing information

2.1 Paper information

- 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.**
- All confidential documents must be stored face down in public areas and should not be left unsupervised.
- Store confidential information in locked cabinets, returning them to these cabinets whenever possible.
- Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.
- Send records you need to archive for statutory, audit or business reasons to the Records Management Service for secure storage, retrieval and, when appropriate, disposal.
- Do not leave paper in resource rooms or by printers where other people may take it or read it accidentally.
- Spoiled photocopies and prints may still be confidential. Do not put them straight into the waste paper bin, dispose of them as confidential waste. Always check that originals have been removed from the device as well as copies.
- Dispose of confidential paper by shredding or put in a confidential waste bag and follow **confidential waste disposal procedure**. Do not dispose of confidential waste in a waste paper bin anywhere else.
- Destroying information earlier than necessary may be a breach of the law so it is important that retention periods are checked before destroying any records.

2.2 Electronic information

- All confidential information must be stored on WCC approved electronic devices or systems with access controlled/restricted, e.g. the WCC network, Google drive with appropriate restricted access, WCC approved systems.
- Confidential information must not be stored on local unencrypted hard drives.
- If confidential information has to be transferred to other portable media, such as USB stick or memory cards, the media must be encrypted with appropriate security software approved by WCC**.**
- PC screens/laptops/tablets must be sited away from public areas so that unauthorised people cannot read the screens, e.g. through windows or while waiting in public areas.

- Notebook PCs, handhelds or any other portable ICT device should not be left unattended in areas accessed by the public (see Mobile Computing below).
- Individual user id/passwords must not be shared with anyone, and do not use anyone else's password. You as an individual are responsible for all transactions undertaken on the WCC network using your network id.
- Passwords must not be written down and left with any equipment or accessible by anyone else.
- Make passwords hard for anyone else to guess by incorporating numbers and mixed case into it. Some systems will force this already.
- Lock Windows PC/laptop 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 while it is unattended.
- Lock phones/tablets using manual lock and use the security settings to lock after inactivity
- If you find you have access to confidential information that you believe should be restricted, you should notify your line manager immediately.

2.3 Storing, retention and disposal

You must comply with legal and regulatory requirements on how long we need to keep information and how to dispose of paper and digital information it at the correct time in a secure manner.

- Make sure information recorded is up to date, complete and reliable.
- Keep a single version of the truth on paper or electronically and do not keep copies of records locally.
- Information must not be kept for longer than necessary and retained and disposed of according to approved WCC Retention Schedules.
- Information should not be deleted to remove evidence or where there is a legal obligation to hold for a period.
- You and your service should know how long personal information is kept for - we have to inform customers and staff of this.'

3. Receiving, sending and sharing information

3.1 Post – receiving and sending

- Internal post within WCC can be used for all types of information.
- Your team procedures should include a single point of mail delivery and handling to make sure there is always someone available to deal with incoming and outgoing post for each team. Post should be opened and dealt with away from public areas and securely, if dealing with confidential

information. Do not leave unsealed confidential documents in open post trays and ‘pigeon holes’.

- Staff must ensure that any mail to an individual marked: Private, Confidential or Personal, or any combination, is only passed to the named recipient unless a prior delegation arrangement has been made.
- If outgoing post contains confidential information to an individual, the envelope should be marked as ‘Private and confidential’ and ‘to be opened by addressee only’. **A return address must be shown on the envelope**.
- Print each customer letter separately making use of any printing security and use window envelopes. Check the address is the current, correct one – don’t copy previous letters. **Double check that the letter and papers are for the correct recipient and address.**
- When using a mailshot or multiple mailings, have a procedure in place to check you haven’t included anyone else’s personal information in the wrong envelope. Another person or supervisor should check mailings against address lists and sign-off before dispatch.
- Consider using signed for/tracked post, if it contains very sensitive, very high risk confidential documents and/or the volume justifies secure delivery.
- Post containing very high risk/Confidential-Restricted information should only be sent to a named person and use of tracked and signed for mail or a courier to deliver to the name person with signature of receipt.
- Where internal mail is being used to send confidential information, the documents must be in envelopes marked ‘Confidential’.
- When internal mail is being transported between Council sites it must be protected from damage or loss.
- If post goes astray or is issued to the incorrect address, notify your line manager immediately and if the information contains personal or confidential information report using the security incident procedure.

3.2 Email – receiving and sending

- The council does not have total control over the emails received, so staff must be aware of the dangers of opening messages from unknown or untrusted sources. **Do not click on links in emails unless you know they are from a trusted source and never provide passwords in response to email requests.**
- If you are not the intended recipient, the sender should be informed that the message has not reached its intended destination and has been deleted.
- Check the email address is the correct one – there are staff with similar names and your email contacts will also have external email contacts. **Double check that the email is for the correct recipient(s) before sending.**

- If sending to a list/group of external contacts/customers, send using 'blind copy' (bcc) so the recipients are not copied in to a large list. **This especially applies to mailshots.**
- Confidential and Confidential-Restricted information **must not be emailed externally using normal email unless**;
    1) the information is encrypted in an attachment using approved software, **or**
    2) it is listed as an WCC approved email address - you must check this list first to see if approved, **or**
    3) you use an approved encrypted email service, e.g. Egress email account, **or**
    4) there is written consent of the recipient (consider equality and disability issues in order to be able to communicate).

- 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. If a permanent record is required they should be saved to the appropriate case file and the email removed. **Do not use personal email as a permanent filing system for customer/ business records.** When a member of staff leaves or moves to another job, the line manager must go through the Leavers Checklist and save and secure any emails needed to be kept as WCC records.
- WCC email must not be forwarded to your own personal email account for private use.

3.3 Telephone calls

- Ensure that you are talking to the correct person that is authorised to deal with the transaction/work by verifying their details. 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 the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation.
- If a message needs to be taken and left on someone's desk, ensure that these messages do not themselves contain confidential information.
- Do not leave confidential messages on an answer machine as these can be reviewed by people other than the intended party.

3.4 Conversations

Staff should remember that even though they may be on WCC premises there may be members of the public, people from other organisations, or external contractors working in an office.

- When having a meeting or interview with someone where confidential 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, confidential 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 public places.

3.5 Redaction and disclosure

If you need to send out information to an individual, it is important that in so doing you do not reveal personal information about other people that should be kept confidential. This is a breach of confidentiality and a data breach and could have serious consequences and possible harm for individuals. Equally, if releasing public information, make sure you have permission to release personal data, or if it is anonymous, there is no personal data or hidden data in the document or dataset.

- Do not use Adobe Reader to redact electronic documents as the original text is still recoverable when sent. **Only use approved redaction software**.
- Avoid paper redactions. If necessary, black out text and copy page, but make sure you cannot see through the blacked out area before release.
- If sending data in spreadsheets, make sure there is no hidden data in cells or tabs. This especially applies where data sets are released to the public and should be anonymous. Remember different software viewers often display hidden data.
- Do not disclose verbally, personal information that the recipient should not know about.
- Do check the identity of individuals before releasing personal information to them.

3.6 Information sharing/processing

The sharing of personal and sensitive information with service partners and other agencies can take place **when**:

- There is recognised legislation that permits this and you are authorised to do so.
- You have the explicit consent of the person to which the sensitive personal information relates.
- The information is anonymised and cannot lead to individuals being identified.

- It forms part of a contractual agreement and is clearly stated within the contract and data processing schedule.
- It forms part of an information sharing agreement/memorandum of understanding/data exchange agreement and the responsibilities are clearly stated.
- You are dealing with an emergency situation and need to prevent an individual from harm (record this on the file/record).

Only share with the relevant people who require the information - keep it on a need to know basis.

3.7 Faxes

A fax machine allows restricted information to be transmitted electronically between locations so needs supporting security procedures to ensure secure delivery.

The ICO, NHS and WCC do not recommended the use of faxes for personal data, as there are more secure alternatives.

Faxes for personal data transmission should not be used. If there is no alternative, then seek advice **and approval** for use of fax to transmit or receive personal data.

4. Mobile working

This includes working away from the office, at home and use of own devices to access WCC information.

Work-related information must not be kept permanently at home, except where authorised for staff whose workplace is their home.

Wherever staff are working on, or in possession of, work-related information they are responsible for it, e.g. in the office, on the phone, at home, en route to or from the office or home, at meetings, conferences, court hearings, etc. 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.

- Take only the confidential papers/files with you that you need and keep out of sight in a bag, do not carry around loose or in clear folder.
- Managers must ensure a log is kept of which confidential paper case files/records staff are taking from the workplace and when they are returned.

- Store confidential paper files/records securely in an envelope or bag. Try to use electronic files on an encrypted device or access via secure connection to the network or approved storage location instead.
- If transferring confidential information/files by hand to a customer/service user or organisation, make sure these are secure in a sealed envelope, handed over to the individual or have a signed-for receipt by an authorised person representing the organisation.
- **By car** - lock away paper files and equipment (laptop/notebook) in the boot, do not leave overnight. Take only the equipment/papers/files with you that you need, leave rest locked away. Delete stored customer/service user personal addresses from sat nav.
- **By public transport** - make sure you take all information and equipment when leaving. Be aware of conversations on mobile phone about confidential information.
- **Own device** - Do not write down passwords/pin numbers. You **must not** use the ‘remember me’ option to save user and password details on your own device when accessing WCC system. Make sure these are unticked and sign out/logout after using a system. Do not save login or passwords if asked. **WCC systems must only be accessed by web access not downloaded apps**, e.g. Google email/drive. Remember any confidential files opened may be downloaded before closing down your device, so delete them from ‘downloads’. If files are not accessed directly (e.g. Google drive format files/WCC EDRM files), then all confidential files must stored and accessed locally via a WCC approved encrypted media.
- **Working at home** - Store paper and equipment securely after use, as you would your own personal valuables. Don’t leave open confidential files on a table. Lock screen on laptop/tablet and close down after use. All confidential information 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. Don’t leave any WCC equipment or information in a car overnight at home, bring into the house and secure. Don’t bin confidential information at home, bring back into an office for confidential waste disposal. Use strong security on a home WiFi connection.

5. Office security

With many different offices and work locations across the council, it is important that the council seeks to maintain a basic standard of physical security at all locations.

- All staff must wear their Corporate ID badge on WCC premises and report losses or thefts immediately to their line managers.

- 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 and display a visitor/contractor ID badge.
- 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 an 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
- 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.

6. Security incidents, breach of data or confidentiality

If staff become aware that information has not been handled according to procedures and there may be a security incident or potential data breach, they must report it to their supervisor or manager immediately.

If you are aware of a potential or actual incident or data breach then please report it by telephoning **01926 73 8881 immediately and in any event within 4 hours**. See: www.warwickshire.gov.uk/imincidents for the WCC procedure.

For losses of equipment or if you believe your email or the network may be at risk, contact the WCC ICT Service Desk immediately on 01926 414141.

If equipment or confidential information has been stolen report to the Police and obtain a crime reference number.

Appendix A Checklist - Information Safe Haven Procedures

Ref	Question	No	?	Yes
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 paper records to the filing system when you are not using them?			
8	Do you lock confidential 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 or use confidential waste bags/bins?			
11	Do you check if papers have personal/confidential information in them, before you bin/recycle them?			
12	Do you know how long you have to keep the records that you deal with?			
13	Do you use the Records Management Service to archive paper records securely, that need to be retained?			
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/laptop sited so that no unauthorised person can see information on your screen?			
24	Do you only store electronic records on the WCC network?			
25	Do you lock your 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 who to report any potential security or confidentiality issues arising?			
31	Do you know where to get further advice if you need it?			