Ref. No.	CO/IG/13
Category:	
People	
Place	
Corporate	Yes
In Constitution	

Confidential Waste, Clear Desk & Screen Policy

Policy Details

What is this policy for?	This policy sets expectations for how anyone who works with Council information should manage their work environment to ensure the confidentiality and security of the information they handle.
Who does this policy affect?	All employees, members, students, apprentices, volunteers, contractors, and other third parties handling council information. It is applicable to all working environments provided by the Council and when working off-site.
Keywords	Clear screen
Author	Lesley Elliott, IT Administrator, Purbeck District Council
Dorset Council policy adopted from	This is a new policy for Dorset Council, which supersedes any sovereign council directives.
Does this policy relate to any laws?	Data Protection Act 2018; General Data Protection Regulation (GDPR)
Is this policy linked to any other Dorset Council policies?	This policy is part of the Information Governance Framework, which also includes: • Information Governance Policy • Data Protection Policy • Data Breach Policy • Individual Rights Policy • Data Protection Impact Assessment (DPIA) Policy • Data Quality Policy • Protective Marking Policy • Records Management Policy • Records Retention Policy • Information Security Management Policy and related standards and protocols
Equality Impact Assessment (EqIA)	An EqIA screening tool was completed and submitted on 5th March 2019. The tool identified that there was no need to complete an EqIA.
Other Impact Assessments	None.

Status and Approvals

Status	Live	Version	1
Last review date	This is a new policy for Dorset Council	Next review date	1st April 2020
Approved by (Director)	Dorset Council Corporate Director: Legal & Democratic	Date approved	February 2019
Member/ Partnership Board Approval		Date approved	

Shadow Dorset Council

Confidential Waste, Clear Desk & Screen Policy

Purpose	*To ensure that all information and data held by Dorset Council, both digitally and as paper records, is kept secure in accordance with the regulatory requirements and disposed off securely at the end of each retention cycle.*
Scope	*This policy covers the way that employees, members and anyone who works with Council information manages their work environment to ensure the confidentiality and security of the information they handle.* *This policy covers all personal, confidential and corporate information that is created, received, managed, shared and disposed of by Dorset Council.* *This policy applies to all employees, members, students, apprentices, volunteers, contractors, and other third parties handling council information It is applicable to all working environments provided by the Council and when working off-site.*

Table of contents

1. Introduction

1.1 Information is one of the core assets of Dorset Council and is vital for the delivery of quality services and the efficient management of resources. Within the Council, we commit to maintaining the confidentiality, integrity and availability of this information. Within this, the Council has a responsibility to safeguard all information in its care, irrespective of the format or medium of storage.

This policy is intended to promote consistent standards for securing information across all office and operational locations in order to: -

- Prevent unauthorised access or use of information, data or records held and processed by the Council.
- Ensure that all information, data and records especially personal or confidential information, is stored securely when not in use.
- Ensure that Information, data or records that are no longer required for legal or business use purposes are securely destroyed.

1.2 It is important that the security of information is also maintained in all locations where council and partner information, e.g. NHS information, is accessed. This is particularly relevant for employees and others that work remotely, including public places such as coffee shops or on trains. Employees need to follow the clear screen / clear desk principles to reduce the risk of compromising information through accidental loss or theft, for example through 'shoulder surfing', i.e. the gathering of information by looking at a computer screen over the user's shoulder.

POLICY DETAILS:

2. Clear Desk Principles

2.1 Dorset Council operates a Clear Desk Policy. The policy is designed to ensure that:

- No information can be accessed by unauthorised personnel; and
- That desks are available for any colleague to work from in accordance with local protocols.

2.2 A clear desk will not contain any information processed by the Council including any information shared with the Council from partner organisations such as the NHS. However, desks can contain the following equipment: a telephone, computer, keyboard, mouse, mouse mat or docking station for laptops and stationery.

2.3 The following principles are provided to help colleagues implement the clear desk policy:

At the end of the working day:

- Computers must be logged off and shut down – refer to the clear screen principles.

- All documents or media with an NHS or Government protective marking, or deemed sensitive or confidential under local arrangements must be secured in lockable office furniture (desk drawers, filing cabinets, cupboards). See the Protective Marking Policy.
- Removable media, where authorised, must be locked away and the key(s) kept in a safe location.

At the end of the working day, employees are asked to:

- Lock cabinets etc. as appropriate.
- Secure laptops and tablets.
- Check that all printed material has been collected from printers and copiers.
- Clear any confidential material, including material on 'white boards' and 'flip charts', from work areas.

2.4 **When leaving your desk at any time during the day, employees must:**

- Lock their computer.
- Clear their desk of any confidential or sensitive material.

3. Clear Screen Principles

3.1 All users should be aware of information security in their working environment, especially if they are temporarily working in public places. When accessing information held by Dorset Council on either corporate or personal devices the following principles apply:

- Computer screens must be angled away from the view of unauthorised persons, especially when viewing any information protectively marked as OFFICIAL – SENSITIVE or NHS CONFIDENTIAL (or identified as sensitive or confidential by local arrangement).
- Screens must be cleared or locked when talking to unauthorised persons.
- All computer terminals must have the auto screen saver set to activate when there is no activity for a period of no longer than 15 minutes.
- Users must lock the screen of their device if they leave their computer for any reason. If they expect to be away from their device for longer than 45 minutes, and at the end of the working day, they log-off or shut down the device and switch off the screen.
- If working in a public place it may be appropriate to use a privacy filters on the screen of your mobile devices, or curtailing what you are viewing.

4. Confidential Waste

4.1 Dorset Council will ensure that confidential waste is protected against accidental loss, damage or unauthorised access until its final destruction by:

- Ensuring that only authorised council personnel or an approved contractor should handle the confidential waste bags.
- Keeping bagged confidential waste secure at all times whilst it is awaiting collection.

- Keeping confidential waste separate from other waste or recycling material. If this is not possible the bags of confidential waste should be clearly labelled.

5. Disposal of confidential and non-confidential waste

5.1 Definitions for Confidential Waste, Confidential Information and Personal Data can be found at Annex A.

5.2 Information that has reached its end of life and is of no historical value should be correctly disposed of. The following procedures should be adhered to:

Non-confidential paper waste:

- Should be placed in recycling boxes, bags or bins provided it does not contain any personal data or confidential information.

Confidential waste:

- Employees should use the correct confidential waste bins, bags or boxes to discard information that is no longer required.
- Information deemed to be highly sensitive should be shredded through a cross cut shredder, as soon as it is no longer needed.
- Once information is in the bin, you must not seek to sift through the bags or retrieve it.

6. Transitional arrangements

6.1 From April 2019, we will be working to bring together teams and services previously managed and operated by different organisations. During this period employees, Members and third parties should:

- Understand the information security risks associated with this period of transition;
- Acquaint themselves with new policies and procedures;
- Understand arrangements for confidential waste disposal at each office;
- Acquaint themselves with how to report a data breach.

7. Roles and Responsibilities

7.1 The following responsibilities apply to all information users with access to council information:

- Employees, apprentices, students and volunteers are responsible for understanding and complying with this policy and associated policies.
    - Failure to comply with this policy or associated policies may result in disciplinary action in accordance with the Employee Code of Conduct, terms and conditions of employment and council disciplinary procedure.
- Managers are responsible for the implementation of this policy and associated policies in their services and teams.
- Members, when handling council information, are responsible for complying with this policy and associated policies in line with the Members' Code of Conduct.

- Agency, contractors, and third party suppliers, when handling council information, are responsible for complying with this policy and associated policies in line with their contract or agreement.
    - Failure to comply with this policy or associated policies may result in the termination of contracts or agreements.

8. Training

8.1 Training will be provided if it is required.

9. Related policies

- Acceptable Use Policy
- Information Governance Policy
- Classification and Protective Marking Policy
- Data Protection Policy
- Data Breach Policy

10. Monitoring and review

10.1 This policy will be reviewed at least annually by the Information Governance Board or following any other changes in legislation, regulations or business practice.

10.2 Proactive monitoring of data breaches by the Information Governance Board may also identify a requirement for the policy and its implementation to be reviewed.

10.3 It is anticipated that Internal Audit will be available to review the implementation of this policy as requested.

ANNEX A

Definitions

Confidential waste *– is information that has reached the end of its life and is due for disposal. It can consist of any of the following: personal data, sensitive personal information, confidential information or any information that has been protectively marked as OFFICIAL-SENSITIVE or NHS-CONFIDENTIAL.*

Confidential information *– is information:*
(a) Furnished to the council by a Government department upon terms (however expressed) which forbid the disclosure of the information to the public;
(b) The disclosure of which, to the public, is prohibited by or under any enactment or by the order of a court; and
(c) Which is not at the time already in the public domain, which has the necessary personal or proprietary qualities to be considered confidential and which was provided to the Council in circumstances imparting an obligation to keep the information confidential.

Personal data *– Is information that can be used, directly or indirectly, to identify a living individual. It is information about someone whose identity is apparent, or can be reasonably ascertained, from the information or a combination of information from different sources. The information can be held in a variety of formats, storage media and locations. For example, fields in a database, CCTV footage, or paper files in a filing cabinet.*