Clear Desk Policy – keeping personal information private

Background

In order for us to provide services, recruit, manage and maintain staff, and work with partners, we will inevitably collect and process personal information – names, addresses, contact details and on some occasions more sensitive information such as banking details and health data. We have a duty to protect the privacy and confidentiality of our staff, members of the public and partners.

We need put in place appropriate arrangements for securing personal, sensitive and/or confidential material (including passwords and login details) and to further develop practices that are consistent and ensure compliance with data protection law.

Private and confidential information

Information can be both private and confidential. For example a completed staff review form is private from almost everyone else in the organisation. The document becomes confidential when it is accessed by others such as HR or your line manager. Staff, partners and members of the public will have an expectation that their personal information will remain confidential unless they have given consent for it to be shared or made public. We are all responsible for protecting the personal data that we legitimately collect and use during the course of our work.

Much of our work doesn't involve the collection and retention of sensitive personal data; however, data that identifies a living individual such as name, signature, email address, is the personal data of the individual that it applies to. It may be possible to combine some information with other information that we hold, perhaps elsewhere in the organisation that allow us to build up a picture of someone including their state of health, whether they are a member of a Trade Union and their political affiliations. Such information, in the wrong hands and published with the consent of the individual, may cause a level of harm and distress that cannot be anticipated – reputational or financial loss, physical or verbal abuse. This may result in a complaint to the Information Commissioner's Office (ICO) and if found to be in breach of the General Data Protection Regulation 2016 (GDPR), a fine of **up to €20 million**. The loss may be easy to measure in terms of monetary value, but not so easy to manage in terms of reputational damage.

Clear desk checklist – things to think about

We need to establish a level of confidence regarding our ability to comply with the policy. We also need to place it in the context of the overall approach to records management – a clear desk policy is one of the key steps in adopting good practice.

The questions below should help you to identify whether you are already compliant, or what you should consider to become compliant.

Private/Confidential Information Audit Questionnaire Checklist

1. **What kind of information do you collect and/or hold?**

   - **Staff**
     Examples
     - Contact information (including next of kin)
     - Financial information (bank account details)
     - Health and sickness records
     - Disciplinary and grievance records
     - Pension information
     - Door access cards
     - Passwords
     - Other – could this be classified as personal information?
   - **Members of the public**
     Examples
     - Contact details
     - Financial information (bank account/credit card details)
     - Witness statements and evidence
     - Details relating to complaints
     - Other – could this be classified as personal information?
   - **Suppliers/partners/other third parties**
     Examples
     - Contact details
     - Financial information (could include contracts and reports)
     - Commercial information (trade secrets/operating procedures)
     - Legal advice
     - Information collected from or about children under the age of 18
     - Other – could this be classified as personal information

2. **Who is the information shared with?**
   - Internally including with members
   - Members of the public
   - Suppliers
   - Partners
   - Other organisations/individuals

   For each of the above think about who you share it with and for what purpose – do you have consent to share, or is there a legal basis for sharing based on a statutory obligation (for example publication of information in connection with planning applications or the names of grant recipients included in our published expenditure report).

3. **How is the information being used/shared?**
   - Only for the purpose for which it was obtained (corresponding with a planning applicant, confirming an event booking, paying a grant recipient)
   - To enable access to the building
   - To enable access to the network
   - Shared with colleagues to ensure that we can provide ‘joined up’ services, or for the protection of staff and members of the public (for example, details of individuals who may pose a threat to the safety of officers when out on site)
   - To market products and services

4. **Where is the information stored?**
    - Is there a hybrid system of paper and electronic records?
    - Do you keep paper files in your office – are these 'live' records (do you refer to them on a regular basis in the course of your daily work)?
    - Are there 'dormant' and historic records related to your area of work held elsewhere in the building? If the answer is 'yes', do you know where they are/do you have an electronic index of this information?
    - Do you store information offsite – if so do you know what and where?
    - Do you take files out of the office (for example to take on site or to work at home)?
    - Do you have information on bits of paper or post-it notes or in diaries which are scattered about your desk or stuck to your computer (is one of these your password?)
    - Do you keep work data on the hard drive (C:\) of your work computer?

5. **How long do you keep the information for?**
    - Indefinitely – don't have the time to review/don't know where to start/don't know what I should be keeping or what can go, or;
    - As long as is needed for the purpose for which it was originally obtained, or;
    - Regularly review and decide what can go, or;
    - In line with our approved Retention Policy, or;
    - In accordance with the Information Management Policies Framework

6. **How is the information secured?**
    - Locked room, only accessible to key holders
    - Locked cupboard, only accessible by key holders
    - Locked desk drawer, only accessible by key holder
    - None of the above – stored on open shelving in unlocked room or sat on desk in office or at home/in car.
    - For electronic files:
        - Stored on network file share such as N:\ drive
        - Stored on home folder (U:\ drive)
        - On work computer desktop
        - On hard drive of work computer (C:\ drive)
        - On home computer
        - On encrypted memory stick
        - On unencrypted memory stick
        - On CD