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 personal information – names, addresses, contact details and on some occasions more sensitive information such as banking details, and health data. We have a duty (and an obligation under the General Data Protection Regulation 2016 (GDPR) to protect the privacy and confidentiality of our staff, members of the public and partners.

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

Private and Confidential Information

Information can be both private and confidential. For example, a completed performance appraisal form is private from almost everyone else in the organisation. The document becomes confidential in the hands of those who have access to it such as HR. There will be an expectation by staff, partners and members of the public that their personal information will remain confidential unless they have given clear 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.

Data that identifies a living individual, such as a name and signature, 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 organization that allows us to build up a picture of someone including their state of health, opinions, religious beliefs and political affiliations. Such information, put into the wrong hands and perhaps published without 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 Commissioners Office (ICO) and if found to be a breach of the 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 measure 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 will 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
- Passwords
- Other – could this be classified as personal information?

☐ **Members of the public**

Examples

- Contact details
- Financial information (bank account)
- Witness statements/evidence
- Details relating to complaints
- Other – could this be classified as personal information?

☐ **Suppliers/Partners/other external organisations**

- 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 Councillors
☐ Members of the public
☐ Suppliers
☐ Partners
☐ Other external organisations

For each of the above think about who you share it with and for what purpose - do you have consent to share, or is the 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 the published monthly expenditure report)?

3. How is the information being used/shared?

- Only for the purpose for which it was obtained (corresponding with an application for an allotment for example)
- To enable access to the building
- To enable access to the network
- Shared with colleagues to ensure that you 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 employees)
- 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 (ie you are regularly referring to them 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 store any information offsite? If the answer is yes, 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 the office or stuck to your computer?
Do you keep work data on your local hard drive (C:\) or on a personal computer at home?

5. **How long do you keep the information for?**

Indefinitely – don't have the time to review/don't know what I should be keeping or what can go, or;
As long as is needed to satisfy the purpose for which it was obtained; or,
Regularly review and decide what can go, or;
In line with our approved Retention Schedule
In accordance with the IT policy regarding password changes

6. **How is the information secured?**

Locked room, only accessible by key holders
Locked cupboard, only accessible by key holders
Locked under drawer cupboard, only accessible by key holders
None of the above – stored on open shelving in unlocked room or sat on desk in office, or at home/in the car
For electronic files:
- Held on network file share (such as N:\drive)
- Held on U:\drive
- On computer desktop
- On C:\drive
- On a home computer
- On encrypted memory stick
- On unencrypted memory stick
- On CD