Privacy Fact Sheet

Handling Information in Your Workplace - Privacy, Security and Records Management Checklist

1. Do you need the information?
   ✔  Confidential or sensitive information requires special attention; if it is not required, don’t collect it.

2. Are filing cabinets containing personal and/or sensitive information locked at night or when not in use?
   ✔  Make one or two people responsible for ensuring the filing cabinets are locked at the end of the day, and responsible for the keys.
   *Hint: If you have highly confidential records, Facilities Management can install bars to additionally secure locked cabinets.*

3. Are printer and fax trays emptied at the end of the day?
   ✔  Make one or two people responsible for clearing the trays at the end of each day.
   ✔  Encourage the use of the secure printing function on printers and multi-function devices.
   *Hint: If unsure how secure printing works, ask your IT support for advice.*

4. Has information been left behind in meeting rooms?
   ✔  Remember to clean whiteboards and remove flipcharts, papers and notes when they contain confidential or sensitive information.

5. Is your department keeping information longer than required?
   ✔  Check the Directory of Records to determine the appropriate retention schedule for your records. *Hint: If you need further assistance, call 8275.*

6. Do staff use shredders and secure bins to securely dispose of documents?
   ✔  Ensure staff are aware of your office secure disposal methods.
   *Hint: Send an email reminder to staff outlining the procedures for disposing of documents particular to your location. If you need further assistance, call 8275.*

7. Are staff aware of who can see their computer screens?
   ✔  Be aware of who can see your screen – either face it away from public areas or add a privacy screen protector.
8. Are PCs locked when staff leave their desks?
   ✓ Use quick keys to lock your screen: Ctrl Alt Delete or windows key and L key. Mac users:
     Command-Option-Eject or Control-Shift-Power (ensure that your Security and Privacy settings
     have the “Require password after sleep or screen saver begins” option enabled).
   ✓ Check screen saver settings that your inactive screen is locked; ask for IT support if necessary.

9. Are diaries and notebooks left open and unattended on desks?
   ✓ Secure diaries when not in use or consider using electronic diaries.

10. Is personal, sensitive or health information left in in-trays over night?
    ✓ Remind staff to lock away confidential documents – promote a clean desk policy.

11. Do staff regularly take large amounts of files or data out of the office?
    ✓ If possible use remote access arrangements (Virtual Private Network) when working from home.
    Use trusted systems such as UVIC supported hardware, computers, systems and email only
    ✓ Only take home (or out of the office) what you really need.

12. Are files visible while in transit?
    ✓ Consider purchasing secure briefcases or folders.
    ✓ Don’t leave files or portable devices unattended.

13. Are portable electronic devices secure?
    ✓ Encrypt USB devices and portable hard drives.
    ✓ Password protect PDAs and smartphones.
    ✓ Password protect and add identifying decals to laptops.
    ✓ When not in use, ensure portable devices are securely stored.
    ✓ And don’t forget to delete information that is no longer needed from these devices.

This checklist can be used in a number of ways:

- Use the checklist to identify privacy risks in a work area or entire location.
- Distribute to individual staff for self-assessment.
- Report results to line management.
- Tally and discuss results at team meetings.
- Communicate the results to staff in a group email or individual emails, to highlight excellent work and where improvement may be needed.
- Use the checklist again in 3-6 months to check on process.