East Dunbartonshire Council

www.eastdunbarton.gov.uk

SOCIAL WORK SERVICES

CLEAR DESK POLICY

Contents

1. Purpose

1.1 **East Dunbartonshire Social Work Services regards its information is an asset which has value. Depending on the nature of the information the value may be monetary or reputational - the effects of unauthorised disclosure could cause serious distress or harm to individuals as well as damaging the reputation of the Council.**

1.2 Information takes many different forms e.g. written / electronic and can be shared in different ways e.g. fax / email / telephone and in how it's stored and moved around (computer / desk / cabinet). What is important is the security and protection of that information in line with legislative around the registration of data handling (handling & movement and individual rights.

1.3 It is the intention of this document to ensure that all information is treated and handled as confidentially and securely as possible.

2. Information Security

2.1 There are 3 key concepts which form the core principles of information security.

1. Confidentiality: Information considered to be confidential, restricted, sensitive or protected must only be accessed by persons who have been authorised to access, use, copy or disclose the information to and only when there is a genuine need to access it.

Example of a breach of confidentiality

Allowing someone to look at your computer screen while you have confidential information displayed if they were not authorised to have or see the information.

2. Integrity: Ensuring information cannot be created / changed or deleted without authorisation. Safeguarding the accuracy and completeness of information and processing methods.

Example of a breach of integrity

An employee accidentally or with malicious intent changes or deletes important information.

3. Availability: The concept of availability means that authorised users have access to information when required and is functioning correctly when the information is needed.

Example of a breach of availability

An employee accidentally or with malicious intent releases a virus on to a computer system which affects access to information.

3. Policy Statement

3.1 To improve the security of information wherever possible East Dunbartonshire Social Work Services are adopting a ***clear desk policy*** for papers, removable storage media (CD Rom, USB, etc.,) and a *clear screen policy* for information processing facilities. This is to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when work areas are left unattended.

3.2 Information security is an ongoing process of exercising due care and diligence to protect information and information systems from unauthorised access, use, disclosure, destruction, modification, or disruption. This Policy will provide clear guidelines for staff on their responsibilities on these areas of potential breach / harm.

3.3 The ongoing commitment to information security will involve ongoing training, assessment, protection, monitoring, and detection, incident response and repair, documentation and review.

3.4 It is also the policy of this service to operate good housekeeping practice. Every office should be kept in a clean and tidy condition and a regular inspection of the premises carried out by the Team Manager / Leader and remedial action taken where necessary.

3.5 For the purpose of this document definitions of information classified **sensitive, CONFIDENTIAL, PROTECTED OR RESTRICTED** is outlined either in terms of the legal requirements detailed in the law, regulations, circulars under section 6 and in the Council policies under section 14 of this policy document.

4. Scope

4.1 This policy applies to **all** permanent, temporary or contracted staff employed by East Dunbartonshire Social Work Services, students and volunteers who can access information under supervision.

5. Principles

5.1 The principles underpinning this approach are detailed below and are to ensure:

- That the security of information is maintained at all times;
- That all legal requirements under such acts / regulations as DPA / HRA / FOI are met for the use / storage / distribution and access of information; this will include appropriate Codes of Practice e.g. SSSC COP for Employers and Employees within Social Services and Council policy.
- Compliance with other Corporate and Departmental Policies.

6. Legislative and Council requirements

6.1 For the purpose of this document, and supporting Social Work Service aim to ensure that all sensitive information will be handled appropriately, the legislative and Social Work Services requirements are defined in:

- The Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Access to Personal Files (Social Work) (Scotland) Regulations 1989
- Circular No: SWSG1 / 89 5493 -6th February 1989 –Code on Confidentiality of Social Work Records

7. Procedure

7.1 Please see Appendices A, B & C

8. Training Implications

8.1 Social Work Services has a responsibility to its staff, service users and all stakeholders to ensure that their details are kept in a secure and confidential environment. This can be achieved through a training and awareness campaign and regular review and update of this and other related policies.

8.2 It is essential that all staff are made aware of the key principles of information security and of the attached appendices. Training on this policy will take place at all departmental levels including through induction of new staff into the organisation.

9. Review / Monitoring Arrangements

9.1 All staff will be responsible for monitoring their compliance with the principles & procedures detailed in this policy; departmental managers and supervisors are also required to monitor and note compliance on a regular basis.

9.2 This policy will be continually monitored and will be subject to a regular review which will take place one year from the date of issue and at two yearly intervals thereafter. The review will be carried out by an officer nominated by the Head of Service.

9.3 An earlier review may be warranted if one of the following occurs:

- As a result of regulatory / statutory changes or developments;
- Due to the results / effects of critical incidents;
- For any other relevant or significant reason.

10. Audit Arrangements

10.1 Each Senior Manager (Children & Families and Community Care) for their respective service will audit compliance periodically on behalf of the Head of Service and report back to the Social Work Management Team their findings.

11. Managerial Responsibilities

11.1 The Head of Service has ultimate responsibility for the compliance of this policy. Senior Manager Children & Families and the Senior Manager for Community Care including members of the Senior Management Team for their respective services are responsible for developing and encouraging good practice in information handling amongst all members of the service.

11.2 The Local Team Managers / Leaders are responsible for ensuring that their staff are trained in, clearly understand, and adhere to this policy. Along with the local Admin Team Leader the Team Manager / Leader must regularly audit, record and monitor adherence of staff to this policy.

11.3 However, it is the responsibility of **all** staff to adhere to the policy's principles and procedures and to the legislative materials underpinning these via the DPA / HRA / FOI and to help maintain the security of information and information systems.

11.4 All staff have a responsibility for reporting breaches of information security incidents to their line managers.

12. Non Compliance

12.1 There is a requirement for all staff to comply with this policy, and where requested to demonstrate such compliance. Failure to comply with this policy will be regarded as a disciplinary incident and will be dealt with under the Council's Code of Discipline.

13. Status of Policy

SOCIAL SERVICES – CLEAR DESK POLICY

Status	Operational
Date of Issue	August 2007
Version	1
Circulation	All staff
Date of Review	August 2008

14. Relationship to other Policies and Procedures

14.1 This policy should be read in conjunction with other East Dunbartonshire Council Departmental Policies on;

- **Corporate - A guide to Public Affairs – Consultation**
- **Corporate Information Classification and Protection Policy (summary)**
- **ICT Security – User Code of Practice**
- **ICT – Internet Access and Email Policy**
- **ICT Disciplinary Procedures _Misuse of I.T. Equipment and Services**
- **ICT – Corporate I.T. Security Policy (Classification Summary)**
- **Social Work Services Communication Strategy**

15. Further Reading

Scottish Social Services Council Code of Practice for Employers and Employees in Social Services.

Access to Personal Files (Social Work) (Scotland) Regulations 1989 - http: / / www.scotland.gov.uk / library / swsg / index-b / c027.htm

Circular No SWSG1 / 89 5493 – 6th February 1989 – Code of Confidentiality of Social Work Records: http: / / www.scotland.gov.uk / library / swsg / index-b / c026.htm

East Dunbartonshire Council Social Work Service – Communication Strategy.

Appendix A

CLEAR DESK PROCEDURE

- Information should be stored on the Corporate Network drive not on the hard drives of local PCs

- Documents either in paper or electronic form e.g. CDs or USBs should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours. Electronic media used must be encrypted.

- Where lockable safes, filing cabinets, drawers, cupboards etc are not available, unattended offices / rooms must be locked to help prevent unauthorised access to information / data in the office.

- At the end of each working day all information which is sensitive, CONFIDENTIAL, RESTRICTED, or PROTECT should be removed from the work space and stored in a locked area. This includes all information which identifies service users, carers and employees. Business information such as contracts, commissioning information and budgetary data are also included.

- Sensitive, CONFIDENTIAL, RESTRICTED, or PROTECT information should be collected from printers immediately.

- Before a service user / carer enters an interviewing area / room all documents relating to previous service users / carers should be removed from view and computer screens cleared.

- Appointment or message books should be stored in a locked area when not in use.

- Reception desks should be kept as clear as possible at all times; in particular information identifying service users should not be held on the desk within reach or sight of visitors.

- The loss of any service user or personal information must be reported to a Senior Manager immediately.

- Any disposal of Sensitive, CONFIDENTIAL, RESTRICTED, or PROTECT information must be in accordance with corporate guidance.

Appendix B

CLEAR COMPUTER SCREEN

- Computer terminals (including laptops) should not be left logged on when unattended and should be locked. Press CTRL+ALT+DEL and select 'lock workstation' to lock your computer.

- Computer screens should be angled away from the view of unauthorised persons.

- The Windows Security Lock should be set to activate when there is no activity for a short pre-determined period of time. (3-5mins). If you need help setting this up contact ICT Service Desk on 8888.

- Users should lock their machines when they leave their desk / room. Where possible other security devices, such as keypads on door entries and exit points should be introduced to areas that are only accessible to staff.

- Only encrypted storage / memory devices must be used to remove information from the Council systems. The use of USB Sticks must be authorised by a Senior Manager. Such devices will be provided by the Council. Staff are not permitted to use their own personal memory devices.

- All memory devices must be returned to the office after use and must not be loaned to anyone outwith the office / department. Such devices must not be left unattended e.g. on a desk.

- External memory devices for example, Laptops, USB sticks, floppy disks, must be treated in the same way as any other form of information, if removed from the office.

- The loss of memory devices must be reported to a Senior Manager immediately

Appendix C

CASE FILE / INFORMATION REMOVAL FROM OFFICE

- Employees should not remove files or information which is Sensitive, CONFIDENTIAL, RESTRICTED, or PROTECT from the office unless absolutely necessary. If so only the relevant documents should be taken and they must be kept securely with the employee at all times.

- Only staff with authorised access to information are permitted to remove it from the office. Information can only be removed for business reasons e.g. business meetings. The information must be kept secure and with the person at all times.

- The removal and return of case file information must be logged in the office.

- Information must only be shared with those who are authorised to have access to it as detailed in this document.

- Information removed from the office must be returned to the office as soon as possible. Information should not be taken out of the office overnight without prior management agreement and proper safety and security arrangements in place.

- Information must be safely and securely packaged prior to being taken out of the office and if transported by car it must be kept out of sight from passers by e.g. locked in car boot.

- The loss of case file information must be reported immediately to your line manager.

Appendix D

East Dunbartonshire Council
Social Work Services

AUDIT PROFORMA

Service: **Location:**

Date of Audit	Compliance with clear desk policy (Yes / No)	If not, please detail what occurred and what action has been taken to ensure compliance with policy.	Is this matter reportable Yes / No	Comments

Signature of Team Leader / Manager:
Date of next review: