

Data Security Policy



ADAM SMITH COLLEGE
INSPIRING LEARNING

Policy Number:	QP1.44
Revision Number:	0
Date of issue:	March 2009
Status:	Approved
Date of approval:	April 2009
Responsibility for policy:	Director Of Corporate Services
Responsibility for implementation:	Director of Corporate Services
Responsibility for review:	Director of Corporate Services
Date of last review:	
Date of last revision:	
Date of next review:	April 2011



1.0 Policy

1.1 Introduction

The College must ensure that the data it collects both in physical and electronic formats is kept secure in order to operate its teaching and business systems and also to comply with its statutory duty in terms of the Data Protection Act 1998. The College has obligations to providers of personal data (students, clients, and staff) under the Act and to protect the College's systems and data from accidental or deliberate damage, loss or corruption.

One of the core principles of the Data Protection Act is that appropriate measures (technical and organisational) must be taken by data controllers (the College) against unauthorised or unlawful access to personal data and against accidental loss or destruction of personal data.

This policy statement is intended to effect implementation of the overall data security policy in respect of data held both in ICT systems and in physical hard copy form

1.2 Ownership and Access to Personal Data

Data is owned by the College. Each significant category of data and management information system is the responsibility of the senior line manager in each area of activity who is accountable for the security of that data and the determination of the staff authorised to access the data.

Responsibility for data security is exercised through the line management structure of the College (Ref: Data Protection Procedure Para 30 and 31)

All personal data is maintained for the purpose defined within the notification under the Data Protection Act. The Data Protection Officer is responsible for maintaining the data protection notification, dealing with formal subject access requests, maintaining awareness of Data Protection legislation and guidelines and offering advice on compliance with the Act.



1.3 Data Access and Disposal

Access to each category of data and management information system is limited to those authorised to access personal data to do their job and system design facilitates and limits such access through a system of permissions, passwords and other security processes. Each member of staff with such access is personally responsible for maintaining the confidentiality of the data to which he/she has access.

1.4 Physical Security

The process of data transfer from physical paper forms (e.g. SR1s) to computerised Management Information Systems (e.g. SITS) shall be carried out in areas that are not open to non-staff members.

Data that is held in physical paper form will be input to the appropriate MIS within defined timescales. These timescales should be as short as possible consistent with business processes. Paper forms will be kept in secure offices or offices with restricted access until they are archived. If paper copies cannot be secured in locked cupboards, they must at least be stored in archive boxes when not being accessed. A clear floor and desk policy must apply.

Archived data will be held in approved archive storage and will be disposed of in accordance with a Records Retention and Disposal Policy (in development).

1.5 ICT Systems

All Management Information System applications are owned by the senior line manager in each area of activity and fall within security and disaster recovery protocols that are administered by the ICT Services Directorate.

Security is an integral part of systems design, the level of security being related to risk as determined by the information owner, having regard to the state of technological development, the nature of the data, user operating needs and cost. ICT Services maintain standards for system security design and for the systems they develop, and are responsible for such design.



They are responsible for ensuring that third party systems are suitable for use on College networks.

ICT Services has in place a Disaster Recovery Plan under which personal data can be recovered in the event of system, hardware or other catastrophic failure.

Application owners are required to sign off acceptance of new systems in order to confirm that operational and security requirements are met.

1.6 Electronic Storage

All personal data must be stored on central storage areas where appropriate security systems are in place to help protect and restrict access to the data contained within (for example SITS).

Personal data must not be held on local hard drives (Laptop or PC) or any portable storage media (CDs; DVDs; PDAs; USB Pen drives). (Ref: Data Protection Procedure paragraph 10).

It is acknowledged that there is a requirement - in the short term - that the College's central staff storage area (commonly referred to as the S: drive) is used for collaboration between different departments. This being the case then no personal information shall be accessible by any person or persons other than those authorised to access and view the data.

The onus is on the initiator to request, from ICT Service's Helpdesk, a folder be set up (on the S drive) so that only named people, which shall be detailed in the request, will have access to said information. The folder will be set up with appropriate permissions and only those named people will have access. As this is purely a short term solution the folder and contents must be deleted when information is passed on satisfactorily.

1.7 Transfer of Data

The transfer of personal data to authorised third parties will be carried out using secure on line systems. The transfer of data by means of portable data storage media must be carried out only in exceptional circumstances and only when the data is secured against unauthorised third party access by an encryption methodology approved by Adam Smith College's ICT Services.



2.0 Justification

This policy ensures that Adam Smith College is compliant with the Data Protection Act 1998, and in particular, the seventh data protection principle that data shall be kept safe from unauthorised access, accidental loss or destruction

3.0 Link to Strategic Plan

This policy contributes to the achievement of Corporate Aim 3 – 21st Century College

4.0 Exemptions

This policy applies principally to college staff.

5.0 Related Procedures

- Data Protection Policy
- Data Protection Procedure
- ICT Services – Disaster Recovery and Business Continuity Plan