1.Title

Information Privacy and Confidentiality

2.Purpose

Management of information (electronic (data) and non-electronic) and administrative proceduresmust ensure that the integrity and quality of information is maintained, that access is properlyauthorised and approved, and that information is used appropriately.

3.Scope

This standard applies to all the Department for Education (the department) employees.

4.Policy detail

4.1 Principle

The department is committed to the principle that information / data required for a government employee to fulfil their function shall be made available to that employee except where such provision is restricted by legislation, policy or security classification of the information/data.

4.2 Data Classification

The department classifies information in accordance with the SA Government ISMF. Where data has been explicitly classified at a higher level of confidentiality (eg Protected or Secret) then the appropriate authorisation is required prior to provision and use of this data. All staff members are responsible for maintaining the security and confidentiality of information to which they have access and/or for which they are custodian, and must keep appropriate records relating to provision of access (refer to 4.6 Freedom of Information).
All information which is yet to be classified is to be treated as For Official Use Only and access to such information must be authorised by the Business Owner.
Refer to the Standard – Information Classification for additional guidance.

4.3 External Access and Information Requests

All requests for access to department information or information systems facilities from external bodies acting under Commonwealth and State legislative provisions, court order or independently must be in writing and must first be directed to the Manager, Legislation and Legal Services who will assess and provide advice and forward to the relevant area of the agency for processing.

4.4 External Use

Where external organisations are authorised to access department information, terms and conditions of use must be agreed, documented and adhered to between the department (including the business owner of the data) and the organisation.

4.5 Release of Information

All decisions to release information to external parties (eg auditors, actuaries, etc) engaged by the department for specific purposes must be approved, documented and controlled by the business owner. Information is released on the understanding that it is used solely for the original purpose. Any subsequent use of the data or any further release must be re-authorised by the business owner.

4.6 Freedom of Information

The Freedom of Information Officer must be consulted regarding requests for the release of information, which are not covered by the normal operational procedures, legislative requirements or the procedures stated in SA Government's *Freedom of Information Act 1991*.

4.7 External Maintenance

External organisations or individuals performing work on department systems facilities must enter into non-disclosure agreements with the department.

4.8 Information Audits

Where the quality of information is critical to the correct operation of a system or may significantly affect business decisions, it is the responsibility of the business owner of the information to establish and maintain a program of cost-effective audits to ensure that the range of the information is within baseline tolerances.

4.9 Data Integrity (Information Systems)

The business owner of the data is responsible for establishing the constraints which ensure the integrity of the data in the system.

4.10 Risk Analysis

All access and use of the department information/data and/or systems by external parties must give consideration of the level of risk and take action in accordance with the departmental Risk Management Policy prior to authorisation and access being granted.