



DATA PROTECTION POLICY

OBJECTIVES

- ensure that information is transferred between the centre and regulation bodies at the appropriate times
- store and disseminate information on regulation bodies qualifications, policies and procedures to all relevant staff
- retain information on candidates, including addresses, in a manner that complies with current data protection legislation 10
- establish if candidates already have UCI or SCN and ensure that these are used for all entries; where necessary, allocate new number to candidates not already registered with appropriate regulation bodies.

1. THE DATA PROTECTION ACT

The Data Protection Act 1998 came into force on 1 March 2000 to bring the UK in line with a European Community Data Protection Directive. The purpose of the Act is to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data. The Act applies to personal data whether it is held on a computer system or on paper. There are particularly stringent rules surrounding 'sensitive' data such as pupil identifiers, pupil characteristics, special educational needs, health, religious beliefs, ethnic background, home address and criminal offences.

Information must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of the data subject
- Held securely
- Not transferred to other countries without adequate protection

2. MANAGEMENT OF EXTERNAL QUALITY ASSURANCE

- staff must understand the process and regulation bodies' requirements
- regulation bodies staff must have access to the centre, sites and electronic assessment systems, as requested by SQA
- the materials must be kept in the right locations and formats, including remote access
- feedback from the external quality assurance must be actioned.

3. INFORMATION FLOW AND RESPONSIBILITIES

regulation bodies Co-ordinator is responsible

- for the distribution of information within the teaching team and parents when required
- for arrangements of secure storage of records and assessment material; and appropriate disposal when no longer required
- for ensuring timely distribution of mail, and any other documentation from regulation bodies , designed to ensure that staff involved in a qualification are kept informed of any matters which affect its delivery and assessment
- for entering candidates for qualifications in accordance with timescales published by regulation bodies
- for ensuring candidates' records are maintained, including information on candidates' progress
- for checking that children, parents and carers information is accurate and up to date. Data collection form to parents/carers is sent on an annual basis.
- in case if there was identified an error in candidates records (i.e. name spelt wrong or incorrect address), the details should be checked against completed by parents data collection form and amended.
- responsible for implementation of recommendations

The Head of the Centre has a duty:

- to arrange regular staff meetings
- to check that staff information is accurate and up to date. Staff should be asked to complete a data collection form upon appointment and encouraged to inform the management about changes in their circumstances
- to update this policy
- to advocate information risk management and raise awareness of information security issues
- to ensure the information is used for the purpose it was collected
- to monitor how information has been amended or added to over time
- to regulate who has access to protected information and why
- **to notify SQA of any changes that may affect the centre's ability to meet the quality assurance criteria, along with details of the types of changes that are required to be notified: changes of**
 - **premises,**
 - **head of the centre, owner, regulation bodies coordinator,**
 - **name of the centre or business**
 - **contact details;**
 - **outcomes of internal/external investigations;**
 - **lack of appropriate assessors or internal verifiers.**
 - **removal of the centre and /or qualification approval by another awarding body;**
 - **centre's arrangements for secure storage of regulation bodies examination papers and candidate evidence (where relevant)¹**

¹ Revision 2024

4. INFORMATION SECURITY

- Users may not remove or copy sensitive or personal data from the school unless the media is encrypted and is transported securely for storage in a secure location.
- Sensitive or personal data must be securely deleted when it is no longer required.
- Computer passwords should not be disclosed or shared between users
- Files and paperwork that identifies individuals must never be left unattended and must be stored in locked cabinets in the Centre office and that must be locked when not in use.
- Documents retention schedules and impact levels are specified in Appendix 2
- All staff processing personal information should be appropriately trained to store and to label documents according to the protection it requires based on Impact Levels:

Impact level	Colour Code	Memory stick?	Example
IL0–Not Protectively Marked	Green	Yes	Newsletters, public information
IL1- Unclassified	Green	Yes	Generic letters to parents containing no personal data
IL2–Protect	Yellow	No	Basic student information such as name and address
IL3–Restricted	Red	No	Sensitive Student information such as ethnicity or FSM status
IL4-Confidential	Red	No	Highly sensitive student data relating to child protection
	Red		

5. INCIDENT REPORTING

Records must be maintained of any suspected breaches of information security using the form in appendix 1. The form will be completed in the event of loss of unauthorised disclosure of information. The details of the incident will be used to amend the current information security procedure and ensure that a similar incident does not happen again.

6. DISCLOSURE OF PERSONAL INFORMATION

Personal information will be disclosed to 3rd parties under the following conditions:

Information sharing with professionals working with children

Information sharing between professionals is vital to ensure the wellbeing of Children. The Centre will follow the “7 golden rules of Information Sharing”:

1. Remember that the DPA is not a barrier to sharing information
2. Be open and honest with the person or family
3. Seek advice if you are in any doubt
4. Share with consent where appropriate

5. Consider safety and well-being
6. Necessary, proportionate, relevant, accurate timely, and secure
7. Keep a record of your decision and reasons

Subject Access Requests for children's and adult's personal information

The request must be received in writing but can be accepted in any format as long as the request clearly identifies the individual. The Centre will respond to the request within 40 Calendar days. If this request comes from someone other than the individual, the Centre must ensure the requester is acting in the best interests of the individual.

A child or young person will always be the owner of their personal information as defined within the Data Protection Act 1998, however if a young person is incapable of making their own decisions which is generally accepted as under the age of 12, the primary carer or guardian would act on their behalf.

Information Security Incident Report Form

Doc No.		Date Opened:		Information Security Incident Report Form
Short Title				
Associated Reference number:		Name and job title:		
Lost <input type="checkbox"/> Stolen <input type="checkbox"/> Other <input type="checkbox"/>				
Impact Risk Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/>				
Has Insurance been informed? Yes/No Date:				
Description of Data lost (Format, Volume, Personal Data, from which system):				
Has the data/system owner been informed? Yes/No Date:				
Name:				
Definition of the Problem and how it was reported, including history of events:				
Impact Summary:				
Detail of Resolution or Workaround:				
Root Cause Analysis:				
Corrective Actions:				
Ref:	Action	Target date	Owner	Complete?
Lessons Learned:				
Ref	Lesson Learned			
Date agreed for Evaluation		Evaluation Date		
Date Closed		The Head of the Centre Signoff		