Data Breach Management Procedure

1.0 BACKGROUND

1.01 As a Data Controller the FE Sector must obtain, manage, process and store all data in compliance with the General Data Protection Regulations (GDPR) and its 6 main principles as per Article 5.

1.02 Article 5(f) of the GDPR states personal data must be:
'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')'

1.03 The College holds a large amount of data / information, both in hard and electronic copy. This includes personal or confidential information (about people), and also non-personal information which could be sensitive or commercial, for instance financial data.

1.04 This procedure will provide staff with guidance should they identify or have suspicion that personal data has been compromised.

1.05 As the Data Controller, the College is accountable for all data being processed as part of the organisational function. It is therefore imperative that a confirmed or suspected breach is reported as soon as possible. Failure to report a breach may result in damage and distress to both the individuals concerned and the College reputation and physical/electronic facilities.

1.06 Failure to report a breach also contravenes Article 33 of GDPR which states:
'In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.'

1.07 The College will provide regular Data Protection training and approved policies and procedures to assist its staff in minimising the risk of theft, unauthorised access, loss and damage while fulfilling their contracted duties.

2.0 SCOPE

2.01 This Standard Operating Procedure applies to College staff and authorised third parties which can include temporary staff and work experience candidates.

2.02 Should a member of staff suspect a breach has occurred, they are responsible for notifying his/her line manager and the College's Data Protection Officer (DPO).

2.03 Once the suspected breach has been reported to the College's DPO, the procedure's scope is limited to the DPO and/or Incident Response Team.

3.0 PROCEDURE

3.01 Definition: What is a Breach?

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Such incidents may be caused by:

- Accidental loss
- Theft
- Human error e.g email containing personal data sent to the wrong person
- Equipment failure
- Damage e.g fire,flood
- Malicous activity e.g hacking

If a data security breach occurs, the College will respond to and manage the breach effectively by means of a 5 part process.

1. Reporting a Breach
2. Containment and Recovery
3. Assessing the Risks
4. Notification of Breaches
5. Evaluation and Response

3.02 Reporting a Breach

Article 33 of GDPR requires the College to notify the ICO of reportable breaches **within 72 hours** of if it being discovered. In some cases the ICO should also be informed of suspected breaches, if significant.

It is therefore critical that once any member of staff or authorised third party have knowledge of a breach, or suspect a breach has occurred they must contact the DPO immediately.

Delays in reporting to the ICO must be accompanied with and explanation of reasons for the delay. The College DPO contact details are:

Carol Anne Deeny
Omagh Campus
2 Mountjoy Road, Omagh
Co. Tyrone
BT79 7AH

CarolAnne.Deeny@swc.ac.uk

Tel: 028 8225 0109 ext. 5434

Should the DPO be unavailable, please contact Mairead Gallagher, Information Security Officer on Mairead.Gallagher@swc.ac.uk or by telephone on 028 8225 0109 ext. 5289

All known details should be included in the initial reporting of the incident. The immediate response will be to establish the nature of the breach and the data involved e.g. has personal data been compromised, what type of personal data and how many individuals may be affected. This will determine which Head of Department will be nominated as the Lead Investigator, the nominee must be notified.

The DPO must report all breaches to the Principal and Chief Executive/College Management Team through agreed internal communications.

The following details of a suspect or confirmed data breach must be recorded in the College register/log:

- Date of Incident
- Time of Incident
- Who Reported Breach
- Due Date of Notification
- Description of Incident/Breach
- Does this incident/breach involve personal data
- Type of Incident
- No. people affected
- Nature of breach
- Description of data
- Sensitive Information
- Category of Sensitive Information
- Risk Rating
- Consequences of breach
- All clients and staff informed?
- Remedial action taken
- All Regulators informed
- ICO Notification Date
- Media Informed
- Case Closed Date
- Further Action

3.03 **Containment and Recovery**

Once details of the breach are known, the DPO will liaise with relevant personnel to contain the effect of the breach. This may include personnel from ICT, Human Resources, College Management Team and Estates; and on some occasions, external suppliers.

The DPO and the department specialists will agree what action must be taken to limit the damage caused by the breach and if possible, restore any lost data e.g. backup tapes. Priority actions may include password changes, disabling swipe access to secure areas within the buildings or searching for lost equipment.

3.04 **Assessing the Risks**

Once the breach has been contained, the DPO and department specialists will assess risks associated with the loss of the data.

See local Data Breach Response Plans for risk scoring.

3.05 **Notification of Breaches**

Where data loss has been confirmed and the risk has been assessed as high, the College is obliged to notify parties affected by the breach.

Notifying the individuals

The DPO and department specialists will establish the identities of individuals whose personal data has been compromised and agree the correspondence to be sent to each subject.

The correspondence should include:

- how and when the breach occurred
- what data is involved
- actions taken by the College
- advice in relation to what steps the individual may need to take to protect themselves in light of their data being compromised e.g. changing a password, cancelling a credit card
- has the Information Commissioners Office (ICO) been informed
- contact name, website link if they need further information in relation to the incident

Notifying the Information Commissioners Office (ICO)

The ICO must be notified of all breaches where large numbers of individuals are involved or where the consequences are serious within 72 hours – the DPO will be responsible for this correspondence.

As per Article 33.2 of GDPR, when notifying the ICO, the information should include, at minimum:

- nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned

- name and contact details of the data protection officer or other contact point where more information can be obtained
- describe the likely consequences of the personal data breach
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The ICO will not normally inform the media of a breach however they may advise the College to inform the media of the breach.

Notifying the Media

Should the ICO advise that the media is informed of the data breach, the DPO will liaise with the Principal and Chief Executive to agree a statement which will be released to the press via the College's Communications and Marketing department, containing all relevant information pertaining to the incident.

3.06 **Evaluation and Response**

While it is critical to contain and assess the risks of a breach, the College must evaluate events leading to the breach and the effectiveness of its response to it.

While carrying out an evaluation the DPO will convene with department specialists, a member of CMT and if necessary seek advice from the ICO regarding what measures the College should and can take to avoid a breach of a similar nature in the future. The College Record of Information Processing should be used a point of reference at this stage.

Considerations should be given to the following:

- Was the breach a result of inadequate policies or procedures
- Was the breach a result of inappropriate training
- Where are documents stored
- Who has access rights to what data
- Has this breach identified potential weaknesses in other areas
- Security of electronic information assets

3.07 **ICO Response**

The ICO will evaluate the data breach and carry out their own investigation into the surrounding circumstances, the nature and seriousness of the breach, and the adequacy of any remedial action taken by the College will be assessed and a course of action determined.

The ICO may:

- Record the breach and take no further action, or
- Investigate the circumstances of the breach and any remedial action, which could lead to:
    - no further action;
    - a requirement on the data controller to undertake a course of action to prevent further breaches;
    - formal enforcement action turning such a requirement into a legal obligation; or
    - where there is evidence of a serious breach of the GDPR, whether deliberate or negligent, the serving of a monetary penalty notice requiring the organisation to pay a monetary penalty of an amount determined by the Commissioner up to the value of €20m or 4% of global annual turnover.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

4.0 COMMUNICATION PLAN

This procedure will be communicated to all staff via Gateway

5.0 REVIEW

This procedure will be reviewed (and amended if required) biannually or sooner to reflect changes in legislation or circumstance.