Data Breach Procedure

Charity Number: SC0 36198

Content

1. Introduction

1.1 The City of Glasgow College holds, processes and shares a large amount of personal data; this is a very valuable asset which we need to look after and protect.

1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.3 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach in the following circumstances:

- whenever any personal data is lost, destroyed, corrupted or disclosed;
- if someone accesses the data or passes it on without proper authorisation; or
- if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

1.4 If the College's data is compromised by a breach, this may result in harm to staff or student data and potentially to the individual(s) whose data is affected, reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2. Purpose

2.1 The College is obliged under the Data Protection Act to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 The law makes it clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the Information Commissioners Office, if required.

2.3 This procedure sets out the process to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the College.

3. Scope

3.1 This procedure relates to all personal and sensitive data held by the College regardless of format.

3.2 This procedure applies to all staff at the College. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the College.

3.3 The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

4. Responsibilities

a. **All staff** have a responsibility for reporting data breach and information security incidents as soon as is possible taking into account the severity of the breach.
b. All staff should report the matter to their line manager and the relevant Director should be made aware of the breach.

Faculty Director or Support Services Directors

a. Responsible for ensuring that their staff have followed this procedure and for ensuring that all relevant information is provided as soon as is practicable to support the breach investigation process.

Data Protection Officer and Director of Corporate Support

a. Responsible with the Vice Principal for Infrastructure for ensuring that any reported breach is investigated and for ensuring that these procedures are followed.

b. Responsible for providing legal and data management advice in relation to the operation of these procedures.

c. Responsible for liaison with the Information Commissioner's Office and for reporting the breach, where required.

d. Responsible for determining the nature and severity of the breach and providing advice to the College on their legal responsibilities in relation to breach reporting etc

Vice Principal of Infrastructure

a. Responsible with the Data Protection for ensuring that any reported breach is investigated and for ensuring that these procedures are followed.

b. Responsible for providing all professional and technical support and risk analysis in relation to the management and containment of any breach.

c. Responsible for ensuring that all appropriate support and technical expertise is provided to the Data Protection Officer in order that the she can determine the nature and severity of the breach and provide advice to the College on their legal responsibilities in relation to breach reporting etc.

Lead Investigation Officer

a. Responsible for leading investigation of the breach (this will depend on the nature of the breach and is likely to be the DPO or a senior member of ICT staff.)
b. Responsible for all duties identified at section 8 of this procedure.

Head of Communications

a. Responsible for providing all professional advice in relation to the management of communications in relation to any data breach and for managing all internal and external communications.

5. Definition/Types of Breach

5.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

5.2. For the purpose of this procedure, data security breaches include both confirmed and suspected incidents.

5.3 An incident in the context of this procedure is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the College's information assets and/or reputation.

5.4 An incident includes but is not restricted to, the following:

a) Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
b) Equipment theft or failure
c) Unauthorised use of, access to or modification of data or information systems
d) Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
e) Sending personal data to an incorrect recipient
f) Unauthorised disclosure of sensitive / confidential data
g) Website defacement
h) Hacking attack
i) Unforeseen circumstances such as a fire or flood
j) Human error
k) 'Blagging' offences where information is obtained by deceiving the organisation who holds it

6. Reporting an incident

6.1 Any individual who accesses, uses or manages the College's information is responsible for reporting data breach and information security incidents to ICT Helpdesk@cityofglasgowcollege.ac.uk. If the data breach involves any personal data then the breach must also be reported to the Data Protection Officer who is the Director of Corporate Support julia.henderson@cityofglasgowcollege.ac.uk.

6.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable taking into account its severity.

6.3 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to personal data, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. See Appendix 1

6.4 All staff should be aware that any breach of the Data Protection Act could result in the College's Disciplinary Procedures being instigated.

7.0 Containment and Recovery

7.1 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

7.2 An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be the DPO or a senior member of ICT staff). This person will be the Lead Investigation Officer (LIO). Their appointment will be agreed by the DPO and the Vice Principal of Infrastructure.

7.3 The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

7.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

7.5 Advice from experts across the College should be sought in resolving the incident promptly.

7.6 The LIO, in liaison with the relevant staff will determine the suitable course of action to be taken to ensure a resolution to the incident.

7.7 The LIO and or the DPO must consider at an early stage whether the Head of Communications should be informed in order to prepare a press release or an internal communication and to be ready to handle any incoming press enquiries. Generally it will be best to forewarn the Head of Communications unless the breach is so minimal and does not affect personal data.

8.0 Investigation and Risk Assessment

8.1 An investigation will be undertaken by the LIO immediately and wherever possible within 24 hours of the breach being discovered / reported.

8.2 The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

8.3 The investigation will need to take into account the following:

a) the type of data involved its sensitivity
b) the protections which are in place (e.g. encryption)
c) what's happened to the data, has it been lost or stolen
d) whether the data could be put to any illegal or inappropriate use
e) who the individuals are, number of individuals involved and the potential effects on those data subject(s)
f) whether there are wider consequences to the breach

9.0 Notification of Information Commissioner's Office and other 3rd parties

9.1 The LIO and / or the DPO, in consultation with the Deputy Principal, will determine who needs to be notified of the breach. Ultimately the DPO must decide whether the ICO should be notified of the breach. You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

9.2 The ICO recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So the law allows you to provide the required information in phases, as long as this is done without undue further delay.

9.3 This means that we must prioritise the investigation, give it adequate resources, and expedite it urgently. If we know that we won't be able to provide full details within 72 hours, it is a good idea to explain the delay and tell the ICO when you expect to submit more information.

9.4 When a personal data breach has occurred, we need to quickly establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then you must notify the ICO; if it is unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

9.5 In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. The ICO will only be notified if personal data is involved. More detailed guidance on when and how to notify ICO is available from the ICO website. For reporting the DPO must complete the standard form https://report.ico.org.uk/security-breach/

9.6 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

a) Whether there are any legal/contractual notification requirements;

b) Whether notification would assist the individual affected – could they act on the information to mitigate risks?

c) Whether notification would help prevent the unauthorised or unlawful use of personal data?

d) Would notification help the College meet its obligations under the seventh data protection principle;

e) The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

9.7 The LIO and or the DPO must also consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

9.8 All actions will be recorded by the DPO.

9.9 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with an appropriate named contact officer in the College who they can contact for further information or support in relation to what has occurred.

10.0 Notification of the individuals whose personal data has been affected by the breach.

10.1 When do we need to tell individuals about a breach?

a) If a breach is likely to result in a high risk to the rights and freedoms of individuals, the law says that we must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

b) A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, we need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

10.2 What information must we provide to individuals when telling them about a breach?

We need to describe, in clear and plain language, the nature of the personal data breach and, at least:

a) the name and contact details of our data protection officer or other contact point where more information can be obtained;

b) a description of the likely consequences of the personal data breach; and

c) a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

11.0 Evaluation and response

11.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

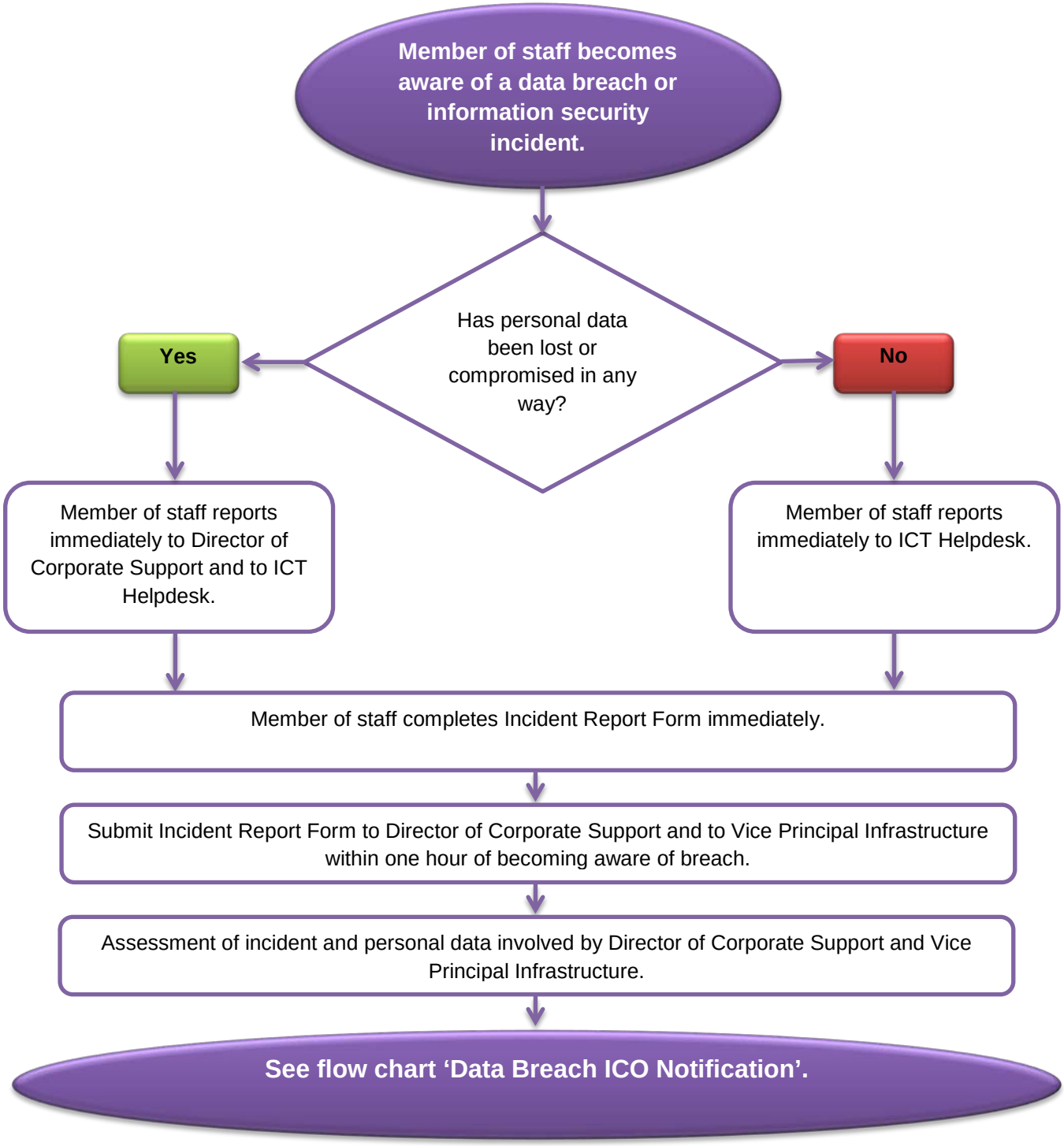
11.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

11.3 The review will consider:

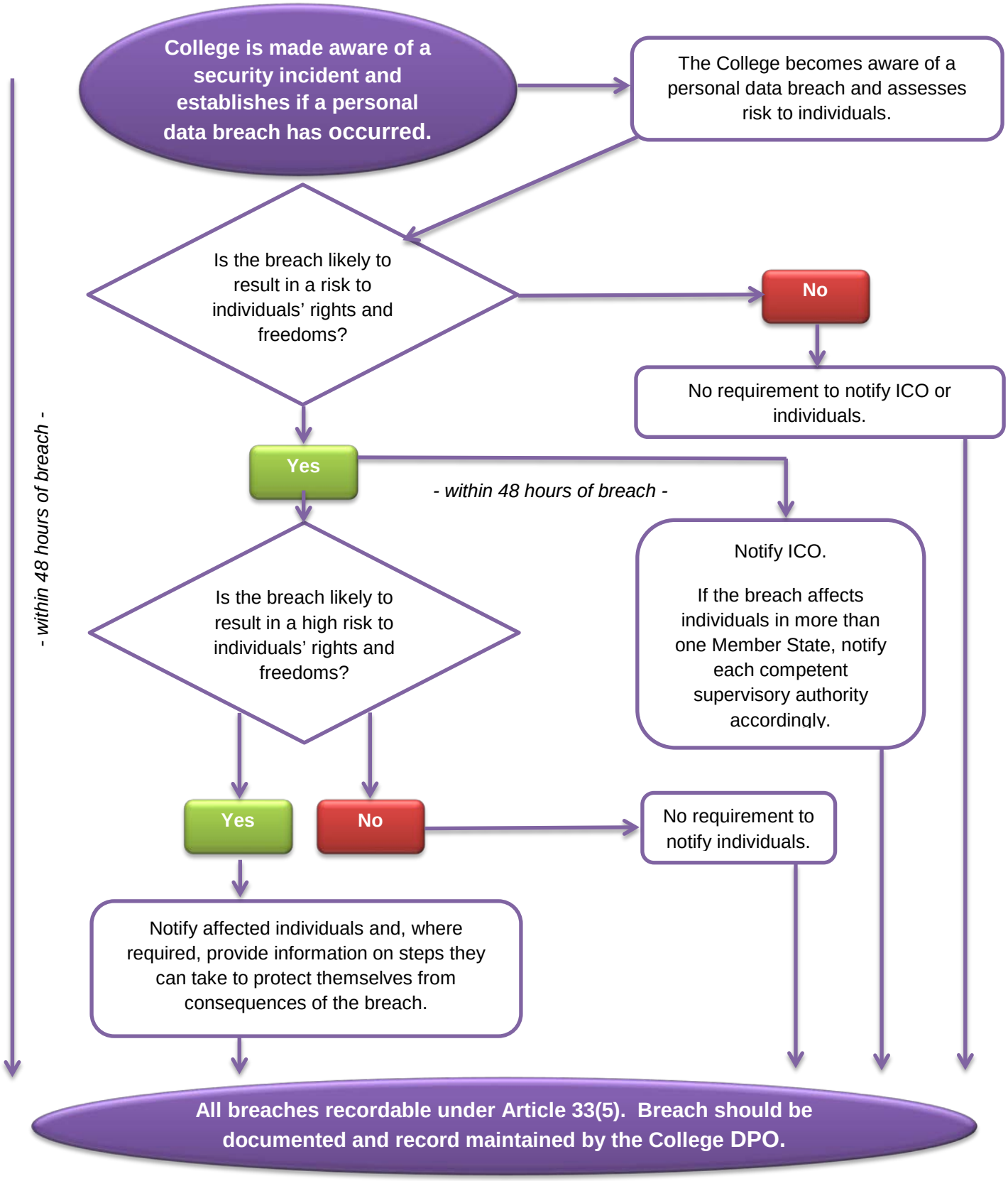
a) Where and how personal data is held and where and how it is stored
b) Where the biggest risks lie, and will identify any further potential weak points within its existing measures
c) Whether methods of transmission are secure; sharing minimum amount of data necessary
d) Identifying weak points within existing security measures
e) Staff awareness
f) Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security
g) If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by College's Senior Management Team and in more serious cases it may be appropriate to report to the College Board or appropriate Committee. Consultation with the College Secretary would be appropriate.
h) whether there are wider consequences to the breach

12. Data Breach Flow Charts

Flow Chart
Data Breach Internal Reporting by Staff



Flow Chart
Data Breach Information Commissioner's Office (ICO) Notification



13. Definitions

Data Protection Officer (DPO): the member of staff with oversight of organisational and technical measures and controls to comply with the Data Protection Act.

Personal Data: data which relates to a living person who can be identified from the data or from a combination of data.

Information Commissioner's Office (ICO): is the UK's independent regulatory body set up to uphold information rights.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Lead Investigation Officer (LIO): Member of staff responsible for investigating a data breach.

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. Please complete Section 1 of this form as soon as possible and email it to the Data Protection Officer julia.henderson@cityofglasgowcollege.ac.uk and ICT Helpdesk ICTHelpdesk@cityofglasgowcollege.ac.uk. If you feel that the breach is serious or you require advice please do not hesitate to contact the DPO for guidance in the first instance. You should also liaise with your line manager and ensure that your Faculty Director or relevant support services Director is made aware of the breach.

Section 1: **Notification of Data Security Breach**	**To be completed by person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number): Brief description of incident or details of the information lost: Number of Data Subjects affected, if known: Has any personal data been placed at risk? If, so please provide details: Brief description of any action taken at the time of discovery:	

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach and if appropriate IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach: Details of information loss: What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the College or third parties? How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	

HIGH RISK personal data
• **Sensitive personal data** (as defined in the Data Protection Act) relating to a living, identifiable individual's
  • racial or ethnic origin;
  • political opinions or religious or philosophical beliefs;
  • membership of a trade union;
  • physical or mental health or
  • condition;
  • sexual life;
  • commission or alleged commission of any offence, or
  • proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	

• Personal information relating to vulnerable adults and children; • Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• student discipline or sensitive negotiations which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed. **Data Protection Officer and/or Lead Investigation Officer** to consider whether it should be escalated to the appropriate Vice Principal or to the Deputy Principal.	

Section 3: Action taken	**To be completed by Data Protection Officer and/or Lead Investigation Officer**
Incident number Report received by: On (date): Action taken by responsible officer/s:	e.g. year/001
Was incident reported to Police?	Yes/No If YES, notified on (date):
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO Notification to data subjects Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details: YES/NO If YES, notified on: Details: YES/NO If YES, notified on: Details:

14 Document Control and Review

Approval Status	**Approved**	
Approved by	**SMT**	
Date Approved	**2 May 2018**	
EQIA Status	EQIA Conducted?	Yes:
Proposed Review Date	2 May 2019	
Lead Department	Corporate Support	
Lead Officer(s)	Director of Corporate Support	
Board Committee	NA	

15 Revision Log

Version Date	Section	Description