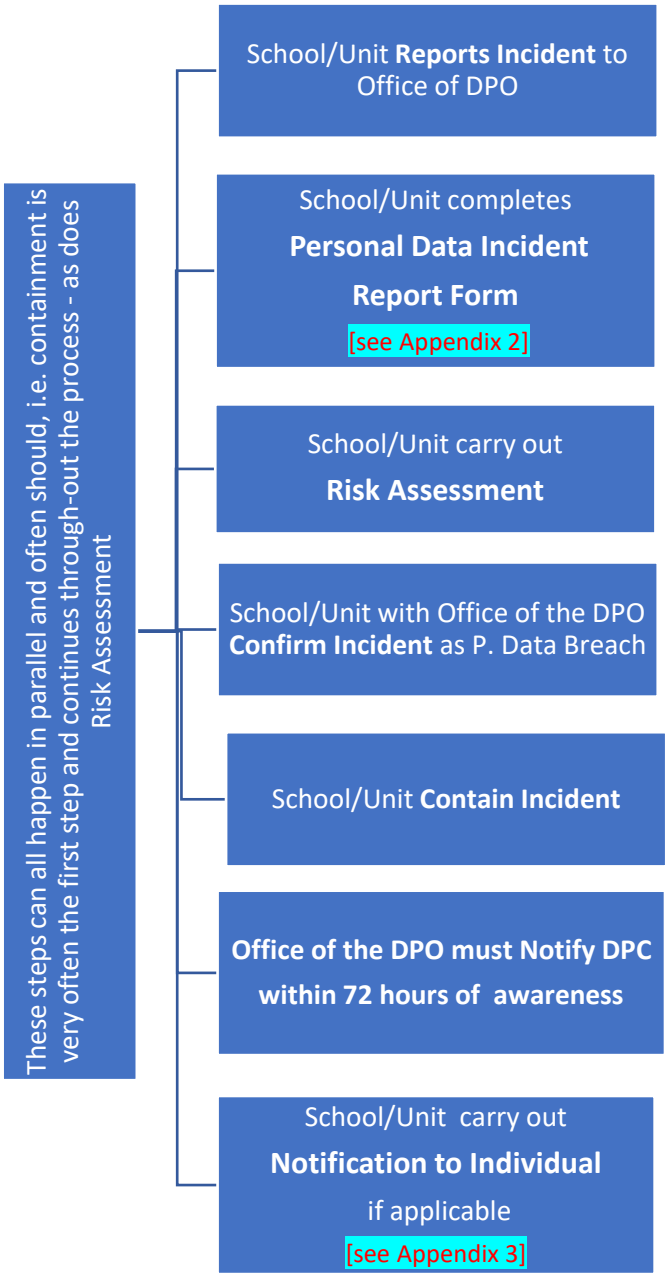
UNIVERSITY COLLEGE DUBLIN GUIDELINES ON REPORTING PERSONAL DATA INCIDENT

CONTENTS:

KEY STEPS FOR REPORTING PERSONAL DATA INCIDENT

In the event of a personal data incident it is vital to ensure it is dealt with promptly to minimise its affect in case it results in a personal data breach. Under GDPR we must notify the Data Protection Commission (DPC) within 72 hours of awareness of a breach and there are penalties for not doing so.



Reporting a Potential Breach?

Please complete the following form

UCD Personal Data Incident Report Form (pdf) / (word)

and send it to

gdpr@ucd.ie

quoting 'Data Incident' in the subject line

For UCD Personal Data Incident Flow Chart [see Appendix 1]

*Data Protection Officer

**Data Protection Commissioner

UCD GUIDELINES FOR REPORTING A PERSONAL DATA INCIDENT

1. INTRODUCTION

For personal data where UCD decides where, when and how they are processed, the university acts as data controller. Controllers are obliged under the Data Protection Acts 1988 to 2018, and the EU General Data Protection Regulation (GDPR), to keep personal data safe and secure, and to respond promptly and appropriately to personal data security breaches. It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality, in order to avoid the risk of harm to individuals, damage to operational business and potential financial, legal and reputational costs to the University.

2. WHAT IS PERSONAL DATA?

Personal Data is any information relating to an identifiable living individual. A person is identifiable if he/she can be identified directly or indirectly, for example by reference to an identifier such as name, address, date of birth, telephone number, account number, job title, photo, IP Address, etc.

3. WHAT IS THE DPO?

The DPO is the Data Protection Officer. The DPO supports the organisation's compliance with GDPR. They have an essential role in acting as intermediaries between the controller, in this case UCD, and the supervisory authorities, that is the Data Protection Commissioner, (DPC).

4. WHAT IS THE DPC?

The Data Protection Commission (DPC) is the national independent supervisory authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. The DPC is the Irish Supervisory Authority (SA) for the General Data Protection Regulation.

5. WHAT IS A CONTROLLER?

GDPR defines a **data controller** as: "a natural or legal person, which alone or jointly with others, determines the purposes and means of personal **data** processing." ... The **data controller** will decide the purpose for which personal **data** is required and what personal **data** is necessary to fulfil that purpose. A data controller shoulders the key responsibility towards the data subject, i.e. the individual whose data is processed and ensures that any personal processing is compliant with data protection requirements. If you are a processor, the **GDPR** places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities.

6. WHO DO THESE GUIDELINES APPLY TO?

- Any person who is employed directly by the University
- Any student who has access to University data in the course of their studies/research
- Any independent contractors, temporary staff or agency staff who have access to University data in the course of their duties for UCD

7. WHAT IS A PERSONAL DATA BREACH?

'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' (Art. 4)

A] TYPES OF BREACH:

***Confidentiality Breach**:* where there is an unauthorised or accidental disclosure of, or access to, personal data.

Integrity Breach: where there is an unauthorised or accidental alteration of persona data.

***Availability Breach*:** where there is accidental or unauthorised loss of access to, or destruction of, personal data.

B] POSSIBLE CONSEQUENCES OF A PERSONAL DATA BREACH INCLUDE:

- Individuals loss of control of their personal data
- limitation of individuals rights
- discrimination
- identity theft or fraud
- financial loss
- damage to reputation
- reversal of pseudonymisation

C] *EXAMPLES OF COMMON UNIVERSITY BREACHES INCLUDE:*

- loss, theft or misplacement of IT equipment or devices containing Personal Data e.g. smartphone, laptop or USB key
- loss, theft or misplacement of briefcase or folder containing Personal Data in physical hardcopy form
- human error resulting in email or post containing Personal Data being sent to an unintended recipient(s)
- unauthorised access to automated or manual Personal Data as a result of a break-in to an office or building on any UCD premises
- unauthorised access to Personal Data held in email or systems as a result of a breach of access controls
- an attack by a "Hacker", i.e. unauthorised access to UCD's computer network, which may consist of a deliberate interruption to IT network services or penetration of the IT network or system, by an unauthorised party with the intention of obtaining information, destroying data or preventing access to data
- unforeseen circumstances such as a flood or fire, in particular where Personal Data is not accessible either temporarily or permanently
- unauthorised access to Personal Data where information is obtained by deception
- in certain circumstances, where there is a loss of access to or availability of Personal Data (temporarily or permanently), for example where Personal Data has been deleted either accidentally or by an unauthorised person and the data cannot be restored.

8. PROCEDURE FOR MANAGING AN INCIDENT

A. IMMEDIATE REPORTING BY SCHOOL/UNIT OF THE INCIDENT TO LINE MANAGER AND THE OFFICE OF THE DPO AS A POTENTIAL BREACH

B. COMPLETION OF PERSONAL DATA INCIDENT FORM BY SCHOOL/UNIT

C. RISK ASSESSMENT BY SCHOOL/UNIT

D. CONFIRMATION OF INCIDENT AS BREACH BY OFFICE OF THE DPO

E. CONTAINMENT OF THE INCIDENT/BREACH

F. NOTIFICATION TO DATA PROTECTION COMMISION BY OFFICE OF THE DPO IF REQUIRED

G. NOTIFICATION TO INDIVIDUAL IF APPLICABLE

NB: The steps above can all happen in parallel and often should, i.e. containment is very often the first step and continues throughout the process – as does risk assessment.

A] IMMEDIATE REPORTING OF THE INCIDENT AS A POTENTIAL BREACH:

Once aware of a personal data incident or potential breach, you must report it to your Head of School/Unit immediately. Acting quickly on this is vitally important as the window for reporting the incident to the DPC is only 72 hours, which includes initial incident investigation and confirmation. Failure to notify on time is itself a breach of the legislation.

B] COMPLETION OF PERSONAL DATA INCIDENT FORM:

In order to establish whether a breach has or has not occurred you or your Head of School/Unit must complete a Personal Data Incident Form and send this on to the Office of the DPO at gdpr@ucd.ie as promptly as possible. [see Appendix 2]

The Personal Incident Form will allow the Office of the DPO understand

- what personal data is involved in the potential breach
- the cause of the breach
- the extent of the breach (how many individuals are affected)
- the harms to affected individuals that could potentially be caused by the breach
- how the breach can be contained.

On completion of the 'Personal Incident Report Form', there will be a short period of investigation carried out by your Business Unit. Your business unit needs to nominate a person to manage this. They will liaise with the relevant schools/units as necessary, to assess whether it is a Personal Data Breach and where they will ascertain the level of risk to the affected individuals

C] RISK ASSESSMENT BY SCHOOL/UNIT:

Once a personal data breach has been established the controller, through the school/unit, must then assess the risk level this breach may have on an individual. The Office of the DPO can play an advisory role in this capacity for you. Depending on the level of risk determined, you may have to communicate the breach to the affected individual, and if so you, are required to do this as soon as is reasonably feasible. (Art. 34). You also need to determine what steps need to be taken to protect the individual.

Determining levels of risk:

Breaches are determined as either low, medium, high or severe.

Low Risk:	individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem
Medium Risk:	individuals may encounter significant inconveniences which they will be able to overcome despite a few difficulties (i.e. extra costs, denial of access to business services, stress, minor physical ailments)
High Risk:	individuals will encounter significant difficulties which they may be able to overcome albeit with serious difficulties (i.e. misappropriation of funds, blacklisting by banks, property damage, loss of employment) or worse still they will face irreversible consequences which they may never overcome (i.e. substantial debt or inability to work, long term psychological or physical ailments)
Severe Risk:	the breach may have a critical, extensive or dangerous impact on affected individuals' reputation or any of the other areas mentioned above

What you need to take into account for your assessment:

- The type of breach that has occurred
- Sensitivity of the personal data
- Number of individuals affected
- Volume of data
- The ease of identification
- The severity of consequences
- The special characteristics of the individual
- The special characteristics of the data controller
- Data unintelligible

These are all outlined in greater detail on the following page. Please keep good records of your approach and how you undertook the risk assessment as well as what steps you carried out, as they may be needed in case of a challenge or questions by the DPC or individuals at a later stage.

- The type of breach that has occurred
  Is it a confidentiality, integrity, availability or malicious breach, as each breach can present a different set of consequences.

  Confidentiality Breach: occurs when the information is accessed by parties who are not authorised or don't have a legitimate purpose to access it.
  Integrity Breach: occurs when the original information is altered, and substitution of data can be prejudicial for the individual.
  Availability Breach: occurs when the original data cannot be accessed when there is a need for it. It can be either temporary loss or permanent.
  Malicious Breach: occurs when the breach was caused by an intentional action as opposed to an error or mistake. Malicious breaches include cases of theft and hacking aiming to harm individuals or may include transfer of personal data to third parties for profit.

- Sensitivity of the personal data
  Usually the more sensitive the data the higher the risk of harm will be. Breaches involving health data, identity documents or financial data can cause harm on their own, - do note a combination of personal data is typically more sensitive than a single piece of data

- Number of individuals affected
  A large quantity of affected individuals influences the overall scale of the breach.

- Volume of data
  A breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

- Ease of identification
  How easy will it be for a party who has access to a set of data to identify specific individuals – is it negligible, limited or significant?

- Severity of consequences
  Where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation individual risk could be severe, particularly if breach concerns data about vulnerable individuals.

- Special characteristics of the individual
  A breach affecting children or vulnerable individuals may place them at a greater risk of danger as a result.

- Special characteristic s of data controller
  i.e. a medical organisation vs newspaper mail-listing.

- Data unintelligible
  If data has been secured with a form of strong encryption and without key compromised, this can substantially reduce the impact to individuals.

D] CONFIRMATION OF THE INCIDENT AS A BREACH BY OFFICE OF THE DPO:

If there is any doubt the Office of the DPO can be engaged at this point also to advise on whether it is a personal data breach or not and can help in determining the risk level. The Office of the DPO will help determine whether: (i) a notification to the DPC; and/or (ii) a communication to the affected individuals is required. If it is established by the Office of the DPO that a personal data breach requires reporting to the DPC, we are obliged to do so within 72 hours (Art. 33). The Office of the DPO will then act as liaison between the DPC and the relevant unit in relation to requests for detailed written reports.

E] CONTAINMENT OF THE BREACH:

While it is being established whether a GDPR breach has occurred, the University needs to take immediate and appropriate action to limit the risk. The business unit needs to advise the Office of the DPO of their containment plan.

Relevant University staff members/managers, will:

- Establish who within the University needs to be made aware of the breach (e.g. IT Services, Buildings & Estates, Legal, Media and Public Relations Office). This information informs what everyone is expected to do to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc.).

- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause (e.g. physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data).

- Establish if it is appropriate to notify affected individuals immediately (e.g. where there is a high level of risk of harm to individuals).

- Where appropriate (e.g. in cases involving theft or other criminal activity), inform the Gardaí.

F] NOTIFYING THE DATA PROTECTION COMMISSIONER BY THE DATA PROTECTION OFFICER:

Under GDPR, the University must report all data breaches to the Data Protection Commission, unless the breach 'is unlikely to result in a risk to the rights and freedom of data subjects' (section 86 DPA 2018). It is the Office of the DPO's role to notify the breach to the DPC no later than 72 hours after UCD's becoming aware of it. Where the University does not notify the DPC within 72 hours the University must include in the notification the reason for not doing so.

The Office of the DPO will have to provide the following information to the DPC:

A) Nature of personal data breach, categories and numbers of data subjects affected, and categories and numbers of records affected.
B) Name and contact details of DPO or other contact points
C) Likely consequences of the breach
D) Measures taken to address the breach and if possible, to mitigate its adverse effects.

G] NOTIFYING THE INDIVIDUAL IF APPLICABLE:

'When the personal data breach is likely to result in a high risk to the rights of freedom of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay' (Art, 34.1)

The main objective of notification to individuals is to provide specific information to individuals about steps they should take to protect themselves. It is your, or Head of Unit's job to notify the individual as the individual's relationship is with you. The Office of the DPO can advise on means of communication and review your communication for you. However, you are best placed to manage your relationship with your employees/students.
A copy/details of your notification should to be sent to the Office of the DPO (gdpr@ucd.ie) for our internal log.

For some helpful examples please refer to Appendix 3

You should also advise the individual that the DPC has been contacted and of their right to complain to the DPC if they so wish. To raise a concern or query with the DPC they can go to following webpage https://www.dataprotection.ie

Guidance on individual notification:

There are a number of ways you can notify the individual:

Formal Letter
E mail message
Telephone call
Website notice
Social media notification
Press/media notification

In general, it is best for the contact to come from a senior manager to demonstrate the seriousness with which you are treating the incident. It is often helpful to make contact by phone and follow up with an email. Depending on circumstances i.e. if the individual resides in a different member state, translation to a local national language may be required.

Your communication must be clear and in plain language and must include the following:

- description of the nature of the breach
- date of the breach so that appropriate steps can be taken by the individual e.g. check relevant accounts since the data was compromised
- the categories and approximate number of personal data records concerned
- the contact name and number of the person who can be contacted for any additional information the affected individual may need. This point of contact must understand the context of the incident and be available first-hand to field any questions the individual may have
- description of the likely consequences of the breach
- description of the measures taken or proposed to be taken by you to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

If individuals are concerned, they can be directed to the Office of the DPO at gdpr@ucd.ie who can discuss the incident more generally with them

Individuals can raise a concern or query with the DPC at any time by going to their webpages here

https://www.dataprotection.ie/en

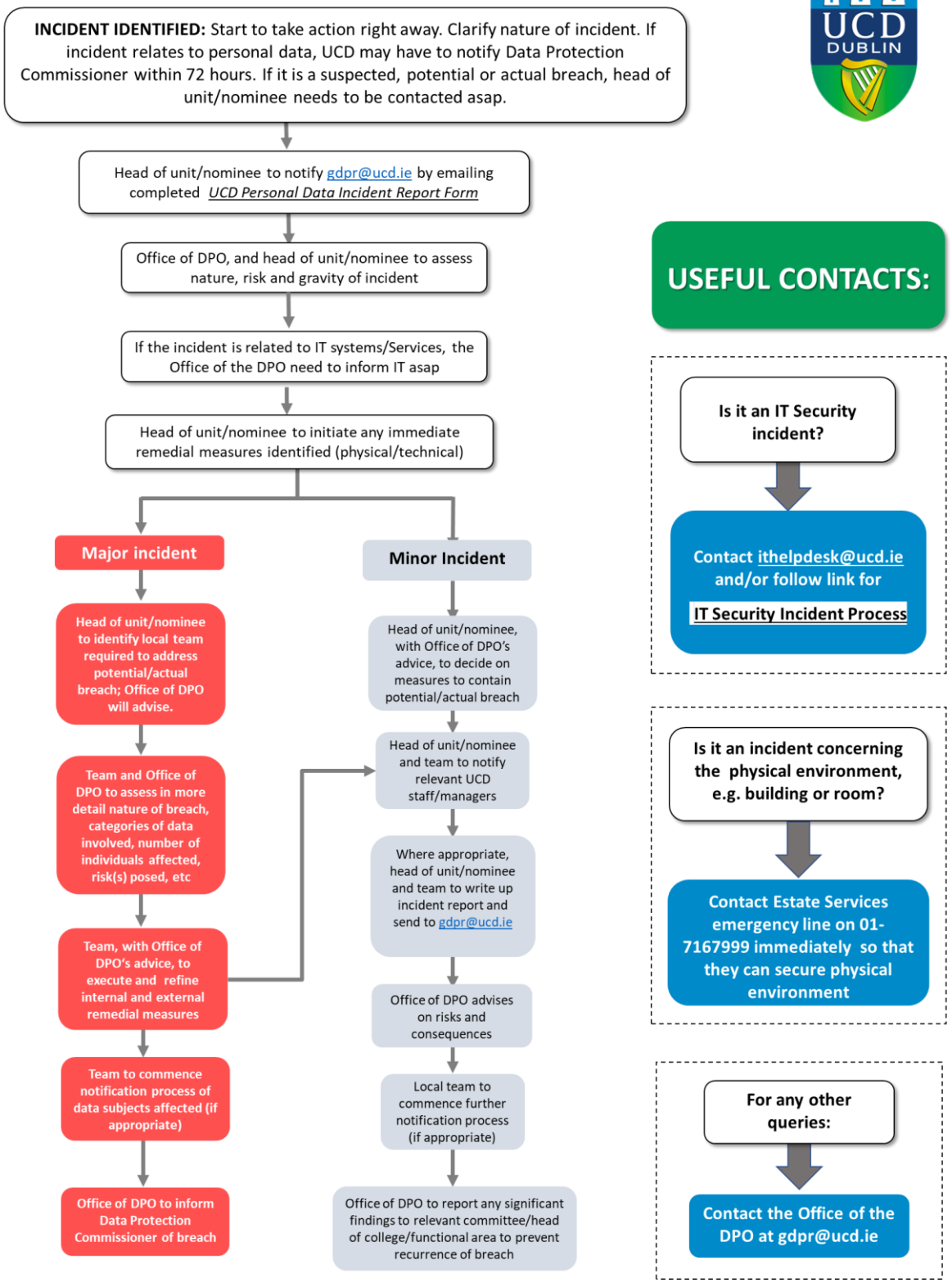
Conditions where the communication to individuals are not required include:

- If measures to protect the personal data were put in place prior to the breach that render the data unintelligible i.e. state of the art encryption
- If steps were taken immediately after the breach was discovered that ensured the recipient of the data did not access it and has deleted/destroyed it, it does not pose a threat

NB: If you use a processor to process your personal data and the processor suffered a data breach, it is the processor's duty to notify you immediately of the breach. As your data subjects are familiar to you, i.e. UCD, but not your processor, any notification in such case should come through you as their data controller.

Appendix 1

UCD Data Incident Flow Chart



Version5._ Dec_2019

Appendix 2

UCD Ref No:

UCD PERSONAL DATA INCIDENT REPORT FORM

In the event of a personal data incident it is vital to ensure it is dealt with promptly to minimise its affect in case it results in a personal data breach. Under GDPR we must notify the Data Protection Commission (DPC) within 72 hours of awareness of a breach and there are penalties for not doing so.

Once aware of a potential breach:

1. You must report it to your Head of School/Unit immediately
2. You must complete the form below or ask your Head of School/Unit to do so (or their delegate)
3. Email the completed form to the Office of the DPO at gdpr@ucd.ie

If you complete this form yourself, ensure your Head of School/Unit reviews it when you have completed it and ensure it is kept updated on the management of the incident.

SECTION 1: INCIDENT TIMELINE	***To be completed by Head of Dept/School/Unit or delegate***
Date and precise time of incident: **[This is when the incident actually occurred]**	
Date and precise time incident was detected: **[This is when UCD became aware of the incident]**	
Date/time of reporting incident to Office of DPO: **[Timely reporting is crucial to satisfy GDPR's 72 hour deadline. If you are reporting outside this time-frame please explain why?]**	
Is the incident on-going?	
School/Unit where incident occurred:	
Name of Head of School/Unit:	
Name of person reporting incident:	
Has Head of School/Unit been informed?	☐ **Yes** ☐ **No**
SECTION 2: ABOUT THE INCIDENT	

Please give a brief written account of what has occurred. Once this is complete you can go through the following 'tick box' questionnaire	
Does the incident involve accidental or unlawful:	☐ **Disclosure of personal data** ☐ **Alteration of personal data** ☐ **Unauthorised access to personal data** ☐ **Loss of access to personal data** ☐ **Physical loss of personal data** ☐ **Destruction of personal data** ☐ **Other (if none of the above please give detail)**
In the case of disclosure, are you aware of any relationship between the affected individual and the recipient of data:	☐ **Yes** ☐ **No** ☐ **Unknown**
If you answered yes to above, please give further detail.	
Which of the following do you think may have caused the incident: (i.e. the nature of the incident)	☐ **Email account compromised** ☐ **Hacking** ☐ **Device lost or stolen (encrypted)** ☐ **Device lost or stolen (unencrypted)** ☐ **Paper lost or stolen** ☐ **Inappropriate disposal of paper** ☐ **Malware** ☐ **Phishing** ☐ **Unintended online publication** ☐ **Network security breach** ☐ **Other (if none of above please give detail)**
How do you think the incident was caused i.e. do you believe the incident to be:	☐ **Employee error or omission** ☐ **Employee intentional act** ☐ **Contractor error or omission** ☐ **Contractor intentional act** ☐ **External error or omission** ☐ **External intentional act**
SECTION 3: ABOUT THE DATA AFFECTED BY INCIDENT	
What identifying details relating to individuals were disclosed? ***(Please do not include any of the personal data itself!)***	☐ **Individual's identity e.g. name, date of birth** ☐ **PPSN or other national ID number** ☐ **Student ID number** ☐ **Identification data (e.g. passports, licence data)** ☐ **Economic or financial data**

	☐ Location data ☐ Criminal convictions ☐ Other (if none of above please give detail)
Do you know the number of individuals affected? ***(Please do not include any of the personal data itself!)***	☐ Actual (Please give number if known) _____ ☐ Approximate ☐ Unknown
Do you know the number of affected records? ***(Please do not include any of the personal data itself!)***	☐ Actual (Please give number if known) _____ ☐ Approximate ☐ Unknown
Are individuals in other EU member states likely to be affected?	☐ Yes ☐ No ☐ Unknown
Were any special categories of data or other highly private data involved? ***(Please do not include any of the personal data itself!)***	☐ Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Membership of a trade union ☐ Genetic or biometric data ☐ Data concerning health ☐ Data concerning sex life/sexual orientation ☐ Data concerning a criminal conviction ☐ Economic or financial data
Were vulnerable individuals affected?	☐ Yes ☐ No ☐ Unknown
If applicable, does the breach involve personal data maintained for the prevention, investigation, detection or persecution of criminal offences or the execution of criminal penalties of the state?	☐ Yes ☐ No ☐ Unknown
SECTION 4: MEASURES IN PLACE BEFORE BREACH, & MEASURES TO RESPOND TO BREACH	
What deficiencies in the organisational or technical measures have been identified as a result of this breach?	
Please explain what mitigating factors will be put in place i.e. is there a need for reviewing processes, retraining, etc. please outline:	
When will these measures be implemented?	
Have you secured/returned the breached data? **If no, please explain why not?**	☐ Yes ☐ No

SECTION 5: CONSEQUENCES/DAMAGES OF THE BREACH FOR THE AFFECTED INDIVIDUALS	
What in your view are the potential consequences of the breach for affected individuals:	☐ Loss of control over their personal data ☐ Limitation of their rights ☐ Discrimination ☐ Reputational damage ☐ Identity theft ☐ Fraud ☐ Financial loss ☐ Others (if none of the above please give details)
Does the breach evaluate/analyse/predict the following (in order to create/use personal profiles):	☐ Performance at work ☐ Economic situation ☐ Location/movements ☐ Reliability/ behaviour/ health ☐ Personal preferences/interests
Considering all the responses to the questions above, how would you now assess the breach: **Severe Risk: the breach may have a critical, extensive or dangerous impact on affected individuals** **High Risk: individuals will encounter significant difficulties which they may be able to overcome albeit with serious difficulties (i.e. misappropriation of funds, blacklisting by banks, property damage, loss of employment) or worse still they will face irreversible consequences which they may never overcome (i.e. substantial debt or inability to work, long term psychological or physical ailments)** **Medium Risk: individuals may encounter significant inconveniences which they will be able to overcome despite a few difficulties (i.e. extra costs, denial of access to business services, stress, minor physical ailments)** **Low Risk: individuals will not be affected or may encounter a few inconveniences, which they will overcome without any problem** **No Risk: device was encrypted so there is no risk to the individual**	***Please read descriptions in left column to help you with your evaluation and please tick below:*** ☐ Severe ☐ High ☐ Medium ☐ Low ☐ No risk
SECTION 6: NOTIFICATION TO AFFECTED INDIVIDUAL	
Have you notified affected individuals of breach:	☐ Yes ☐ No
If yes, how: ***Can you please send a copy of this to the Office of the DPO (gdpr@ucd.ie) for their records?***	☐ Formal letter ☐ Email message ☐ Telephone call ☐ Website notice ☐ Press/media notification

Appendix 3

Below are two sample 'notification' letter. An initial phone-call would be advised, and a letter e-mailed thereafter. Please feel free to use these as a guideline but modify to satisfy your incident or circumstances ensuring you have covered all the legal requirements above. If in any doubt you can contact and consult with the DPO (gdpr@ucd.ie) to seek advice on informing the individual and on the appropriate message to be sent.

Sample letters of Individual Notification:

Dear

[advise individual of why you are contacting them]

We are writing to inform you of a recent personal data breach that occurred in UCD in (Name of school/area) on (Date). We want to assure you that you are in no way responsible for this incident, but we are contacting you as we are aware that you are among the individuals affected by it.

[outline in clear, plain language what has happened and date it occurred]

On (Date), an email was sent out notifying individuals of (x). The recipients of this email should have been entered into the 'bcc' field, but in this case the 'cc' field was used in error, so unfortunately your personal data was made visible to all other recipients. If you have not already opened this email, we would ask you to please discard it. If you have opened it, please delete it immediately. We should advise you to respect the privacy of all involved and remind you that you do not have the right to use the personal data for any purpose in the future.

[explain measures they may need to take to protect themselves if applicable or measures taken by the unit to ensure this does not happen again]

Following this incident, we have reviewed our internal procedures and implemented changes to reduce the risk of reoccurrence. Our team all receive GDPR training, but a refresher course has been organised as a result of this.

[let them know you have contacted DPO/DPC if applicable and give them relevant points of contact]

We have advised the Office of the DPO of this incident and they in turn have reported it to the DPC. If you would like to discuss any details of this further please don't hesitate to contact me at the below number, or equally the office of the DPO at gdpr@ucd.ie. Should you wish to raise a concern you can by contacting the DPC on http://www.dataprotection.ie/en/individuals/raising-concern-commission

[apologise for inconvenience]

Please accept our sincere apologies for any upset or inconvenience caused.

Yours sincerely,

_____

Dear

Further to [reference call], I would like to reiterate our sincere apologies for this data breach and the potential exposure caused to you.

One of our email accounts was breached on [date of breach]. UCD IT Services became aware of suspicious activity and suspended the account on [date breach detected]. The device was then examined to determine if the data breach posed a threat to either UCD or any of its students. During our investigation it was discovered that a small number of credit card details were present in the email account.

As discussed, as a precautionary measure, we recommend that you review your recent transactions to satisfy yourself that there are no unauthorised transactions on your account. Furthermore, we recommend that you contact your card supplier and advise them of the potential issue, asking them to cancel and reissue your card ending XXXX. In the event that you find any unauthorised transactions from [date of breach] on your account please advise your card supplier of these immediately.

Any record containing your card details will be destroyed in an appropriate manner thus ensuring no such exposure remains.

Should you incur any costs in checking credit files please advise us and we will address these directly with you.

***Please contact [contact details etc.] if you would like more information about this incident**.*

We have notified the Data Protection Commission of this incident. If you are still not satisfied with the response, you can raise a concern or query with our DPO, or with the DPC, by going to their webpages here

https://www.dataprotection.ie/en

Once again, our deepest apologies for this breach

If you could advise us of receipt of this mail it would be much appreciated

Yours sincerely

For further information please refer to the DPC's guidance about breaches at
https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification
or refer to Article 29 Working Party Guidelines on Risk Assessment
https://ec.europa.eu/newsroom/document.cfm?doc_id=47741