UCG Data Breach Report and Assessment Form

Who is involved?

Start by identifying who is to be involved in dealing with the breach. This will include both internal staff involvement and the use of external data breach experts, IT consultants and others.

Internal Personnel

Role	Name	Email
[Data Protection Officer OR Data Protection Manager**]**	GRCI Law	dpoaas@grcilaw.com
[Other **[**director OR partner OR manager**]** responsible**]**		
[Data Breach Team Manager**]**	Data Privacy Team	gdpr@ucg.ac.uk
[Head of IT**]**	Paul Hardman	paul.hardman@cwc.ac.uk
Other personnel involved (e.g., Head of Finance if accounts data compromised, Head of HR if employee data compromised).		

External Personnel

Organisation	Expertise/Purpose	Individuals involved (if known)

Details of the Incident

Provide details of the incident so far as they are known at this stage.

Question	Additional notes
Date of breach/suspected breach:	*This may be the actual date of the breach if known or the date upon which the breach was discovered if not known.*
Date breach discovered:	*If different from the date of the breach.*
Date breach notified to organisation/manager:	*If different from date breach discovered.*
Reason for notification time gap:	*If there was a period of time between discovery and notification to management, explain why that time occurred.*
Is the breach ongoing?	*If known at this stage, is it a one-off breach or a breach that is continuing?*
Person notifying breach	*Who discovered the breach and who notified it to management if different? Provide details of their role within the organisation e.g., IT manager, personnel manager etc.*
How did the breach come to light?	*What factors led to the person reporting becoming aware of the breach?*
What is the nature of the breach?	*Describe the breach in outline terms e.g., hacking, inadvertently sending data to the wrong recipient, theft of hardware etc.*

Initial Assessment of Breach

As soon as possible after the report is made, carry out an initial assessment of the breach and its implications for the organisation and data subjects.

Question	Additional notes
Describe the nature of the breach	*Provide a summary of the facts surrounding the breach so far as they can be ascertained at a preliminary stage.*
Describe the implications of the breach	*Does the breach affect:* • *Confidentiality: disclosure of, or access to, personal data?* • *Availability: loss of access to, or destruction of, personal data?* • *Integrity: alteration or partial destruction of personal data?*
Responsibility for the breach	*Is it possible at an early stage to ascertain who was responsible for the breach, e.g., external hackers, disaffected staff member, staff member responsible for loss of equipment, file, or data etc?* *Was the person responsible the person who reported the breach?*
Types of data affected	*Describe the data that is the subject of the breach e.g., customer records, email addresses, username/passwords, paper-based files, employment records etc.*
Approximate number of data items/subjects affected	*Either the number of pieces of information or the number of data subjects.*
Sensitivity of the data affected	*Is the data very sensitive, e.g., usernames and passwords, personal information about customers, health records, or less sensitive data e.g., publicly available information?* *Other factors include:* • *Ease with which data subjects can be identified.* • *Was data encrypted and was decryption key compromised by breach.* • *Severity of consequences for data subjects.* • *Special characteristics of the data subjects or the organisation.*

Remedial Steps

Having identified the nature of the breach what preliminary steps are to be taken to contain or remedy the breach?

Question	Additional notes
What steps need to be taken to contain the breach?	*E.g., if the breach is an online threat taking the network offline, if the breach is a staff member taking steps to revoke their access to their network.*
Can the breach be remedied using internal personnel only?	*Can the organisation resolve the matter without calling in external help?*
If external assistance is required, identify the assistance needed.	*E.g., data breach experts, network consultants, the organisation's IT support company etc.*
Does the organisation have Cyber or other relevant forms of insurance?	*If yes, ensure that they are informed at as early a stage as possible so that remedial costs are covered by insurance.*
Can lost data be retrieved?	*Take care that if malware is involved that backups are not tainted with the malware.*
Does hardware need to be replaced?	*Has equipment been stolen or compromised to such an extent that new equipment is needed?*

Detailed Assessment of Data

A full review needs to be undertaken as to the data affected, the data subjects whose data it was and the sensitivity of the data. This will need to be recorded.

Question	Additional notes
What types of data were involved?	*List all types of data including the categories of data and the approximate number of records affected.*
How sensitive was the data?	*For each type/category of data you will need to assess the sensitivity of that data since this will to a degree determine what follow up steps need to be taken.*
Which data subjects are affected by the data?	*This needs to be determined for each type/category of data as it will affect the follow up. In particular, were any of the data subjects in a vulnerable position, e.g., children, vulnerable adults, those for whom data relating to special category information was held.*
Calculate the likely consequences	*Work out the consequences of the breach on data subjects, either by category/group/type or, if necessary, individually.*
Was the data affected either encrypted or anonymised?	*If encrypted the strength of the encryption and the likelihood of its breach needs to be calculated. If the data was anonymised, the likelihood that individual data subjects can be identified needs to be calculated.*
What has happened to the data?	*If the data has been lost or stolen, then attempts need to be made to ascertain whether it could be used to the detriment of the data subjects. If it has been damaged or destroyed, can it be recovered?*
Is this breach related to other breaches and if so, how?	*Is this a one-off breach or does it form part of a pattern? If there have been previous breaches, why were they not dealt with in such a way as to prevent future beaches?*
Are there wider ramifications of the breach?	*Could the breach be linked to long term criminal activities, are there any security implications or could the breach be linked to terrorism.*
Are there likely to be operational consequences for the organisation?	*Can the organisation continue to function following the breach? Has compromised data been able to be recovered?*

Notifications

Various parties will need to be informed of the breach depending upon its nature, severity and the sensitivity of the information in question.

Question	Additional notes
Does the data breach need to be reported to the police, e.g., did it involve theft or fraud?	*Not all data breaches will involve criminal activity, e.g., accidental loss or destruction will not be a police matter.*
Does the Information Commissioner's Office need to be informed[2]?	*The ICO must be informed of a personal data breach except where it is unlikely to result in a risk to the rights and freedoms of data subjects. Where necessary, notification must be made without undue delay and, where possible, not later than 72 hours after the breach became apparent. If not possible then reasons for the delay must be provided within 72 hours. If in doubt, make a report.* *Factors to consider include the potential harm to data subjects, the volume of the data involved and the sensitivity of that data.*

Question	Additional notes
Do the data subjects need to be informed[3]?	*Data subjects should be notified of a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to their rights and freedoms to allow them to take the necessary precautions. They should be told the nature of the personal data breach as well as recommendations for mitigating potential adverse effects.* *The notification should be made as soon as possible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.*
Consider additional factors in determining whether to inform data subjects.	*These factors may include:* • *Was the data encrypted or anonymised so that although there was a breach, the identity of individuals would not be disclosed?* • *Have subsequent steps been taken to ensure that there is unlikely to be an impact upon data subjects (e.g., all account logins changed)?* • *Would there be a disproportionate effort in informing individuals when compared with the danger to them?* • *Are you under a contractual or other legal obligation to inform data subjects?* • *Did the breach involve sensitive data?*
Should you be notifying any professional bodies that the breach has occurred?	*E.g., the Solicitors Regulation Authority if you are a law firm or the Financial Conduct Authority if you are a financial services business.*
Do any third parties need to be notified	*E.g., a data controller if you are a data processor.*

Looking to the future

Lessons need to be learned from the breach and steps taken to prevent a future breach from occurring.

Question	Additional notes
Preliminary conclusions as to reason the data breach occurred	*Why did the data breach happen e.g., negligence of staff, accidental loss, theft, malware, inadequate processes and safeguards, hardware failure?*
Had steps previously been taken to prevent breaches of this nature?	*Did the organisations have policies and safeguards and had these been followed? What security measures existed in relation to this?*
Why did safeguards fail to prevent the data breach?	*Were there shortcomings or was it deliberate?*
What steps are to be taken to put right the shortcomings if any?	*Identify where processes and policies are inadequate and make them stronger.*
How will policies and processes be tested for adequacy in the future?	*How can you know that remedial steps are adequate?*
Does hardware/software need to be replaced/updated?	*Check for currency of patches and upgrades.*
Is staff training required to ensure future issues do not arise?	*Policies and processes are only of use if they are known about, and their importance appreciated.*
Does a data privacy risk assessment need to be undertaken?	*A review of the whole organisation, the department affected or specific processes.*

Question	Additional notes
Is external assistance required on an ongoing basis?	*If personnel in the organisation lack a skill set, does it need to be brought in from outside?*