UCG Data Breach Management Policy

This policy describes how the College manages data breaches (for City of Westminster College and the College of North West London).

Document Status	
Owner	Amanda Thorneycroft
Author	Gora Selliah
Date of Origin	December 2024
Colleges covered	City of Westminster College, College of North West London
Version	0.1
Date of Approval	09 December 2024
Date of Next Review	December 2027
Approval Body	UCG Corporation

Introduction

1.1 Changes in the way in which technology is used and applied throughout United Colleges Group (the **organisation**, **we**, **us**, **our**) means that there is an increasing number of ways in which data security breaches, whether as the result of human error or malicious intent, can occur. Given the confidential and often sensitive nature of the data that we hold and process, this can present a major problem.

1.2 We obtain, use and retain personal information (**personal data**) as part of our day-to-day activities. That personal data relates to current, former and prospective staff, students, suppliers, and third parties (**the data subjects**). In doing so, we are subject to various legislative and regulatory provisions including those set out in the United Kingdom General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA18**). These address how we, as data controllers and data processors, should obtain, deal with, and retain personal data. We are committed to complying with our legal and regulatory obligations to manage personal data in an appropriate manner and to being concise, clear, and transparent about how we obtain and use personal information and how (and when) we delete that information once it is no longer required.

1.3 To help us take a responsible approach to the protection of the data with which we deal, and to ensure that we comply with all the regulations and legislation that we are subject to, we need to have in place a robust and systematic process for responding to any reported data security breach.

1.4 This policy has been implemented to provide that robust and systematic process and it should be followed by all staff to ensure that a consistent and effective approach is in place for managing any data security breach and other information security incidents across the organisation.

1.5 This policy applies to everyone and to all data and information, regardless of format, including (but not limited to) information relating to staff, former staff, prospective staff, applicants for posts within the organisation (whether successful or not), students, contractors, third parties, those to whom marketing information has been sent and data processors acting on behalf of the organisation. It should be read in conjunction with other relevant policies implemented by us including our Data Protection and Data Subject Rights policies.

1.6 By adopting a standardised and consistent approach to all reported incidents and by ensuring that any such incidents are managed in accordance with best practice guidelines, we aim to ensure that:

1.6.1 All incidents are reported in a timely manner and properly investigated.

1.6.2 All incidents are handled by appropriately authorised and skilled personnel.

1.6.3 The appropriate staff are involved in dealing with any incident that arises.

1.6.4 All incidents are recorded and documented.

1.6.5 The full impact and other implications of the incidents are understood.

1.6.6 Steps are taken to mitigate any damage caused to us or our staff, students or other third parties and that further damage is prevented.

1.6.7 Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny.

1.6.8 External bodies, authorities, regulators, and data subjects are informed as necessary.

1.6.9 All incidents are dealt with in as timely a manner as possible and normal operations are restored as quickly as possible.

1.6.10 The incidents are reviewed to identify improvements in policies and procedures for the future.

1.7 All staff must take time to familiarise themselves with this policy so that they know what is expected of them in the event of a data security breach.

What is a Data Security Breach?

2.1 A data security breach is defined in Article 4(12) of the UK GDPR as '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'.

2.2 In other words, a data security breach is not limited to circumstances where the organisation has been hacked into or targeted by outside forces. It is any situation where personal data that is held or controlled by us is actually or potentially accessed and/or used by those who should not be accessing and/or using it, or not able to be accessed and/or used by those who should be accessing and/or using it.

2.3 Thus, a data security breach is about more than just losing personal data. It applies to a whole range of circumstances which can lead to the destruction, loss, alteration, unauthorised disclosure of, access to or use of personal data and can include:

2.3.1 The loss of a data stick or laptop with personal information on it.
2.3.2 The theft of a paper file with personal data in it.
2.3.3 A hacking incident.
2.3.4 The failure of a system which prevents data from being accessed.
2.3.5 Malware which locks users out of certain data or corrupts it so that it is no longer usable.
2.3.6 User error causing data to be inadvertently deleted.
2.3.7 Actions by any person to corrupt or delete data.
2.3.8 Hardware failure such as a hard drive upon which data is stored no longer being accessible.
2.3.9 Inadvertent access to data whilst it is being used in a public place.
2.3.10 Data on a screen or file on your desk which has been seen by unauthorised personnel or clients.
2.3.11 Insecure disposal of files and or technology.
2.3.12 Sending the wrong information to the wrong person in an email or having an email intercepted.

2.4 For the purposes of this policy data security breaches include both confirmed and suspected incidents. Staff who believe that they may have inadvertently caused a data security breach should, therefore, report that breach.

2.5 Data security breaches may take many forms. However, the more common forms are:

2.5.1 **Threats to confidentiality**: we handle confidential and sensitive data on behalf of students and hold personal and employment data about staff and third-party contractors. Threats to confidentiality is high on the list of events against which we wish to guard. These events may include:

(a) Attempts to gain access to information by third parties and other unauthorised persons through the process of hacking, malware, phishing, and fraud.

(b) The intentional passing of restricted information by those who have authority to access it to others who do not.

(c) By the inadvertent disclosure of information to someone not entitled to that information, for example by the inclusion of the wrong attachment to an email or the sending of an email to the wrong recipient.

2.5.2 **Threats to integrity**: we rely on the data which we hold being accurate and up to date. As a result, any error, intentional act or natural or accidental event that can result in the corruption or loss of any information held or used by us can potentially lead to a failure on our part to best represent the interests of students or staff and third-party contractors.

2.5.3 **Threats to availability**: the critical nature of timing for many of the actions which we undertake means that having access to the right data at the right time is an imperative part of our everyday work. Events, whether deliberate or accidental, which cause disruptions in processing or loss of stored or transmitted information can therefore be particularly problematic for us. Threats to availability can take the form of wilful damage, power failure, procedural errors or theft, malicious software (including denial-of-service attacks) and other dangers to our data and operating system such as viruses, worms, spoofing and email spamming.

Reporting Security Breaches

3.1 All personnel must be ever vigilant about data security breaches, and potential data security breaches, and must report them at the earliest possible opportunity to the Data Privacy Team (gdpr@ucg.ac.uk) using our UCG Data Breach Report and Assessment Form.

3.2 Details of security incidents can be very sensitive and like all sensitive information it must be handled with discretion and only disclosed to those who need to know the details. Please, therefore, do NOT discuss the disclosure, or the events leading to it, with anyone else in or outside the organisation other than the Data Privacy Team (gdpr@ucg.ac.uk).

3.3 It will be the function of the Data Privacy Team (gdpr@ucg.ac.uk), either personally or through an appointed assistant, to determine whether the information submitted constitutes a data security incident or data breach and it is they who shall determine how it is to be dealt with in accordance with the appropriate security breach procedures. Staff must not attempt to conduct their own investigations, unless authorised to do so, in order to ensure that evidence is not destroyed and that matters are dealt with proportionately and expeditiously.

3.4 The handling of data security breaches is subject to strict time limits which, if not observed, could cost us a substantial amount by way of fines, loss of business, loss of resources and reputational damage. It is imperative, therefore, that reports of data security breaches are made as a matter of urgency.

3.5 Staff must provide whatever information and assistance is reasonably required by the Data Privacy Team (gdpr@ucg.ac.uk) to facilitate the speedy conclusion of the investigation.

3.6 The data breach or security incident will be concluded when the investigation is complete. The member of personnel making the report may or may not be informed of the outcome of the investigation depending upon the sensitivities and need for confidentiality.

3.7 All staff must always be aware of the potential for the media and press to want to find out about a data security breach. Any member of personnel experiencing an attempt by a third party to obtain information about the data security breach must pass the enquiry on to the Data Privacy Team (gdpr@ucg.ac.uk) WITHOUT FURTHER COMMENT OR EXPRESSING ANY OPINION ABOUT THE MATTER.

Handing Data Security Breaches — Overview

4.1 Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident.

4.2 The UK GDPR requires that data security breaches are dealt with as expeditiously as possible and that details of the breach are reported to the Information Commissioner's Office (**ICO**) without undue delay and ideally within 72 hours of us becoming aware of it (unless the breach is unlikely to result in a risk to the rights and freedoms of those whose data is being processed). If the notification cannot be made within 72 hours then the ICO must be given a reason for this within 72 hours. Failure to do so could result in us becoming liable to pay a fine.

4.3 Data security breaches can require substantial time and resources to rectify. The following procedure outlines the main steps in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently.

4.4 Throughout the breach management process, records should be kept of what action has been taken, why it was taken and by whom the action was taken. An activity log must be kept together with copies of any correspondence, emails and records of telephone conversations relating to the breach. In addition, the following data should be recorded:

4.4.1 The date and time the breach occurred.
4.4.2 The date and time the breach was discovered.
4.4.3 Who/what reported the breach.
4.4.4 Description of the breach.
4.4.5 Details of any ICT systems involved.
4.4.6 Any other substantiating material.

4.5 The Data Privacy Team (gdpr@ucg.ac.uk) will have authority to:

4.5.1 Conduct whatever enquiries he/she/they reasonably believe are necessary to establish the nature and cause of the breach and the extent to which data has been compromised.
4.5.2 Take whatever initial steps are necessary to contain the breach.
4.5.3 Make internal reports and recommendations and subsequent remedial plans to ensure that similar breaches do not occur in the future.
4.5.4 Determine who within the organisation needs to be made aware of the breach, to identify who will be involved in assisting them in restoring the data, protecting the interests of the organisation and its students, staff and third-party contractors, handling the breach and carrying out all subsequent steps needed to deal with the breach.
4.5.5 Inform, as appropriate, the ICO, the police, our insurers and any other competent body or authority.
4.5.6 Inform, as appropriate, the data subjects affected by the breach and to provide them with details of a point of contact within the organisation, the likely consequences of the breach and the measures being taken, or proposed to be taken, to address and mitigate the breach.

Handling Security Breaches — Implementation

5.1 The primary duty of the Data Privacy Team (gdpr@ucg.ac.uk) is containment and recovery, to minimise the impact of the breach and use his/her/their best efforts to get everything back to normal as soon as possible.

5.2 The Data Privacy Team (gdpr@ucg.ac.uk) must ascertain the nature of the breach, what needs to be done to contain the breach so far as possible and begin the task of recovering any lost data. The specific actions taken will depend upon the nature of the breach.

5.3 If the breach involves some form of breach of cybersecurity, damage to hardware or software or some other technical problem which is outside the range of skills of those within the organisation, then the Data Privacy Team (gdpr@ucg.ac.uk) should appoint an approved contractor to assist in dealing with the incident.

5.4 The Data Privacy Team (gdpr@ucg.ac.uk) should then assess the potential risk arising from the data security breach. In doing so, he/she/they should consider:

5.4.1 The nature of the information or data involved.

5.4.2 The sensitivity of the information or data involved.

5.4.3 Any security mechanisms in place (e.g., passwords, encryption).

5.4.4 What has happened to the data—has it been lost or stolen, and could it be used to the detriment of the data subject?

5.4.5 What the information or data could convey to a third party about the data subject.

5.4.6 The number of individuals affected by the breach.

5.4.7 The harm that could come to those individuals as a result of the data security breach.

5.4.8 The extent to which there are wider issues to consider, e.g., risks to the public generally or risks to the reputation of the organisation or others.

5.4.9 Whether individuals' bank details are involved and if so, whether and which banks need to be informed.

5.5 The Data Privacy Team (gdpr@ucg.ac.uk) will carry out all necessary notifications. Generally, a report should be made to SLT (Senior Leadership Team) as to the nature of the breach and the steps that have been taken to deal with it. The Data Privacy Team (gdpr@ucg.ac.uk) needs then to consider whether other notifications are necessary.

5.6 In deciding whether notification is required, the Data Privacy Team (gdpr@ucg.ac.uk) will want to consider the following:

5.6.1 Are there any legal or contractual requirements? Service providers have an obligation to notify the ICO in certain circumstances, in other areas sector specific rules may point towards issuing a notification.

5.6.2 Can notification help the organisation meet its security obligations?

5.6.3 Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information provided to mitigate risks, for example by cancelling a credit card or changing a password?

5.6.4 Are a large number of people affected, or are there likely to be very serious consequences?

5.6.5 Does the data security breach involve particular groups of individuals, for example children or vulnerable adults?

5.7 Finally, the Data Privacy Team (gdpr@ucg.ac.uk) will wish to carry out a thorough review of the event and will need to consider:

5.7.1 The action that needs to be taken by the organisation to reduce the risk of future breaches and minimise their impact.

5.7.2 Whether policies, procedures or reporting lines need to be amended to increase the effectiveness of the response to the breach.

5.7.3 Whether there are weak points in security controls that need to be strengthened.

5.7.4 Whether all staff are aware of their responsibilities for information security and whether they have been adequately trained.

5.7.5 Whether additional investment is required to lessen exposure and if so the resource implications.

5.8 The Data Privacy Team (gdpr@ucg.ac.uk) should put any recommended changes to policies and/or procedures into a report to SLT (Senior Leadership Team) who should implement those recommendations as soon as possible.

Training

6.1 We will ensure that all staff receive adequate training as to their data protection responsibilities and as to how to act and respond in the event of a data breach. Those whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to a breach, will receive additional training to help them understand their duties and how to comply with them.

6.2 Information will be provided to all new staff as part of their induction training.

Failure to Comply

7.1 We regard compliance with this policy as an extremely serious matter. Failing to comply puts at risk those individuals whose personal information is being processed, carries the risk of significant civil, criminal, and regulatory sanctions for us and our personnel and may, in some circumstances, amount to a criminal offence by the individual.

7.2 Because of the importance of this policy, any failure to comply with provisions set out in this policy by any staff will be taken seriously and may lead to disciplinary action being taken against that person under our usual disciplinary processes. Breaches may result in dismissal for gross misconduct for employees and immediate contract termination for non-employees.

Review and Update

This policy will be reviewed and updated annually or more frequently, if necessary, to ensure that any changes to the organisation's practices/business plan are accurately reflected.

Appendix 1

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?*

Question	Additional notes
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.*

Question	Additional notes
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.*
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*

Question	Additional notes
	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.*
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?*