PERSONAL DATA BREACH POLICY AND PROCEDURE

Effective for all staff, students, visitors and contractors

Policy category:	Technology and Data Protection
Approved by:	Policy Review Group 27/03/26
Policy owner:	Data Protection Officer
Related policies:	Data Protection Policy and Procedure
Applicable to:	Staff, students, visitors, contractors
Effective from:	27/03/2026
Date review date:	30/03/2028

Document Version Control 1.0 – Revision History

Section	Summary of changes	Date updated
1	Update and reinforcement of legislation	27/03/2026
Throughout	Update from BTC to College Group, update of email address and job titles, update of Information Commissioner title	27/03/2026
6	Updated section about staff training	27/03/2026
8	New flow diagram in addition to how to guide. Confirming that data breaches can be reported to IT helpdesk as well as the DPO.	27/03/2026
9	Additional section about disciplinary	27/03/2026

Contents

1. Introduction

1.1 The UCS College Group is committed to compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Digital Use and Access Act (2025). These regulations govern the processing and protection of personal data by the College Group, and this policy sets out the approach to managing personal data breaches in accordance with these legal and contractual obligations.

1.2 A personal data breach is defined 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."

1.3 The cause of a data breach can be accidental, or deliberate. This definition means that a breach is about more than just the loss of personal data. Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid compromise security privacy.

1.4 A compromise of information security, confidentiality, integrity or availability may result in harm to individual(s), organisational or personal reputational damage, a detrimental effect on service provision, legislative non-compliance and/or financial penalties imposed by the Information Commissioner.

1.5 The College Group needs to have in place a robust and systematic process for responding to any reported data security breach to ensure it can act responsibly and protect information assets as far as possible.

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

1.7 Types of incident include, but are not restricted to:

- Loss of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, iPad, tablet device or paper record)
- Careless document storage, display or retention leading to confidential personal data being visible to others on screen or on paper
- Equipment theft or failure

- System failure
- Unauthorised use of, access to or modification of data on information systems
- Attempts (failed or successful) to gain unauthorised access to information on IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation

2. Aim of the Policy

2.1 The aim of this policy is to standardise the College Groups' response to any reported data breach, ensure they are appropriately logged and managed in accordance with best practice guidelines, ensure any breaches are contained, risks associated with the breach minimised and actions considered to secure personal data and prevent further breaches.

2.2 This policy applies to all College Group information, regardless of format, and applies to all staff, students, visitors and contractors acting on behalf of the College Group.

2.3 By adopting a consistent approach to all reported incidents it will ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are managed by appropriately authorised and skilled staff
- Appropriate levels of College Group management are involved in response management
- Incidents are recorded and documented
- The impact of an incident is understood and action is taken to prevent further damage
- Evidence is gathered, recorded and maintained in a form that will withstand both internal and external scrutiny
- As appropriate, data subjects or external bodies are informed

- Timely management of incidents with minimal disruption to operation
- Incidents are reviewed to identify policy or procedural improvements.

3. Responsibilities

3.1 All staff and volunteers are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly where urgent action is needed to prevent further damage.

3.2 Managers are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

3.3 The Data Protection Officer (DPO) is responsible for overseeing management of the breach in accordance with the Data Breach Management Plan.

4. Data Classification

4.1 Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore, it is important that the College Group is able to quickly identify the classification of the data and respond to all reported incidents in a timely and appropriate manner.

4.2 All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following categories:

Public – any information published or available publicly (in the public domain)
Internal – any information circulated within the College Group only, including information which is only accessible to certain employees/groups/committee members/contracted parties
Confidential – any personal or confidential information
Protected – highly sensitive information.

5. Data Security Breach Reporting

5.1 Confirmed or suspected data security breaches should be immediately reported to the **Data Protection Officer** dpo@ucscollegegroup.ac.uk Under the data protection legislation any confirmed or suspected high level data security breaches must be

reported to the Information Commissioner (IC) within 72 hours (non-working hours) of the College Group becoming aware of the incident. In the event it is not possible to investigate a breach fully within 72 hours, the DPO will report as much information as possible, explaining the delay and submit further information as soon as possible. The DPO will give the investigation adequate resources and expedite the process as a matter of priority.

5.2 The report to the IC must include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. This information will include:

- A description of the breach including where possible the categories and approximate number of individuals concerned
- The categories and approximate number of personal data records accessed
- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, including where appropriate the measures taken to mitigate any possible adverse effects

The Data Breach Incident Report Form (Appendix 1) must be completed as part of the reporting process.

5.3 Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who will be responsible for managing the incident (Appendix 2).

The incident will be investigated to determine whether a breach has occurred, by establishing whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

5.4 The investigating manager (appointed by the DPO) will consider the likelihood and

severity of the resulting risk. If there is a likely risk then the DPO will notify the Information Commissioner. If the risk is unlikely then the incident will be documented but not reported. This will be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress) through:

- Loss of control over their data
- Discrimination
- Identity fraud or theft
- Financial loss
- Unauthorised reversal of Pseudonymisation (for example key coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

5.5 The breach will be documented, irrespective of whether the breach is reported to the Information Commissioner. For each breach this will include the:

- The facts and cause of the breach
- Any effects thereof
- Action taken to minimise the breach and ensure as practicably as possible that it does not happen again (such as establishing more robust processes or providing further training for individuals)

The Breach and Near Miss Log will be stored on the College Groups network, with restricted access.

6. Data Breach Management Plan

6.1 The management response to any reported data security breach will involve the following four elements. See the Data Breach Checklist (Appendix 3).

a. Containment and Recovery
b. Assessment of Risk

c. Consideration of Further Notification

d. Evaluation and Response

6.2 Each of these elements will be conducted in accordance with the Data Breach Checklist. An activity log recording the timeline of the incident management will also be completed (Appendix 3).

6.3 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will notify those affected without undue delay. This will help them to take any necessary steps to protect themselves from the effects of a breach. The notification will include:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

6.4 The DPO will provide regular, documented training to all staff on data protection responsibilities and breach reporting procedures. Training records will be maintained and reviewed annually to ensure ongoing compliance and awareness.

6.5 Governors will be informed of any data breaches on a termly basis through the Audit Committee, or sooner where a significant breach has occurred.

7. Evaluation

7.1 It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of the College Groups response to it and the remedial action taken.

The following table is used to evaluate the severity of an incident.

Evaluation of Incident Severity

Highly Critical: Major Incident	**Contact**
• Special category data/sensitive information • Breach involves > 1000 individuals • External third-party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response beyond normal operating procedures	Incident Lead: DPO Other contacts: Other Senior Management Team (SMT) members as required External parties such as police, Information Commissioner (IC), individuals affected
Moderately Critical: Serious Incident	**Contact**
• Confidential data/information • Not contained within the College Group • Breach involves > 100 individuals • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Immediate response not required • Incident response may require notification to SMT	Incident Lead: DPO Other contacts: Other SMT members as required
Not Critical: Minor Incident	**Contact**
• Internal or confidential data/information • Breach involves < 100 individuals • Risk to College Group low • Inconvenience may be experienced by individuals impacted • Loss of data/information is contained/encrypted • Incident can be responded to within working hours	Incident Lead: DPO Other contacts: Other SMT members as required

8. What to do if you discover a data breach

8.1 Don't panic! You know it's happened, so you're already taking control of the situation. You must report the breach to the Data Protection Officer (DPO) immediately by emailing dpo@ucscollegegroup.ac.uk and IT helpdesk, 01278 441247 or using the online SharePoint form.

8.2 All breaches big or small, regardless of the harm or the potential harm, should be identified and reported.

IDENTIFYING AND REPORTING A DATA BREACH

If you discover a data breach, you must report this to our **Data Protection Officer (DPO**) immediately The Data Protection Officer is **Emma Kilner**. Contact on 01278 441247 for any breach or suspected breach dpo@ucscollegegroup.ac.uk or using the online form on SharePoint, or via the IT helpdesk

False alarms or breaches that do not cause any harm to individuals or to the College Group should nevertheless be reported as it will enable to the College Group to learn lessons in how to respond and the remedial action that we put in place.

We have a legal obligation to keep a register of all data breaches. Please ensure that you report any breaches, even if you are unsure if it is a breach or not.

BECOMING AWARE OF A DATA BREACH – INVESTIGATING

We become aware of data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data or security being compromised. From this point, our time limit for notification to the **Information Commissioner (IC)** will commence.

When you report a data breach to the **DPO**, they will promptly investigate the breach to ascertain whether we are fully aware that a breach has occurred leading to personal data being compromised for our data subjects.

The investigation will be done within 48 hours of a breach being reported to the College Group, so that it can ensure it complies with the **72 hour** deadline to report any data subject or serious security breaches in a timely way to the IC data breach may result
in disciplinary action.

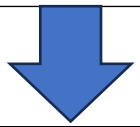
ASSESSING A DATA BREACH

Once you have reported a breach and the DPO has investigated it and has decided that we are aware that a breach has occurred, DPO will log the breach in our Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity.

Once the level of severity is known, the DPO will notify management. If necessary, they will appoint a response team which may involve for example our HR and IT teams

and we will assign responsibility for particular tasks as necessary across the response team. We will then investigate the breach and consider any on-going risks to the College Group and any individuals affected.

If the DPO and management consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us.



FORMULATING A RECOVERY PLAN

The DPO and senior management will investigate the breach and consider a recovery plan, if required, to minimise the risk to individuals. As part of the recovery plan, the DPO and senior management may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

NOTIFYING A DATA BREACH TO THE IC

Unless the breach is unlikely to impact on data subjects or result in a risk to the rights and freedoms of individuals, we must notify the breach to the IC within **72 hours** of becoming aware of the breach. **We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.**

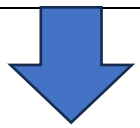
The content of the notification will be drafted by the DPO, and any notification to the IC must only be made by the DPO.

NOTIFYING A DATA BREACH TO INDIVIDUALS

We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our DPO in line with our procedures and in conjunction with consulting the IC if considered necessary. We will notify individuals in clear and plain language and in a transparent manner (for example by email, SMS or letter). **Please be aware that under no circumstances must you try and deal with a data breach yourself.**

In some circumstances, we may not need to notify the affect individuals. The DPO will decide whether this is the case.



NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES

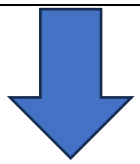
We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

- Insurers
- Police
- Employees
- Parents/Guardians
- Sponsors
- Banks
- Contract counterparties

The decision as to whether any third parties need to be notified will be made by our DPO and senior management. They will decide on the content of such notifications and act within 5 days of becoming aware of the data breach.

UPDATING NOTIFICATIONS

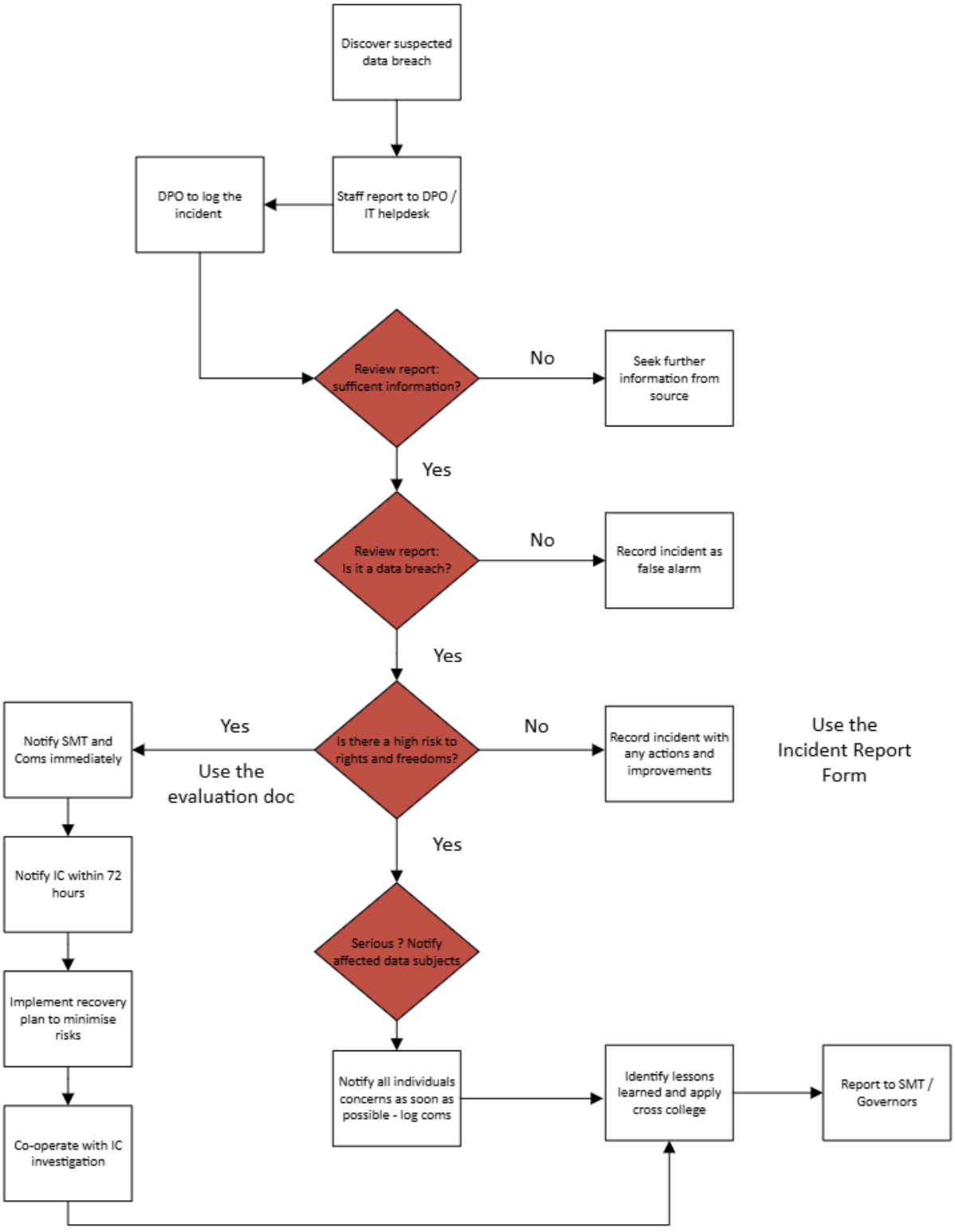
We need to keep the IC up to date about the data breach. If anything changes from the time we send the initial notification to the IC, our DPO will consider whether we need to update the IC about the data breach



EVALUATION AND RESPONSE

The key to preventing further incidents is to ensure that the College Group learns from previous incidents.

It is extremely important to identify the actions that the College Group needs to take to prevent a recurrence of the incident. Our DPO and the Senior Leadership Team will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register. Senior management may then make changes to College Group procedures to minimise the likelihood of incidents occurring again.


Discover suspected data breach
Staff report to DPO / IT helpdesk
DPO to log the incident
Review report: sufficent information?
No
Seek further information from source
Yes
Review report: Is it a data breach?
No
Record incident as false alarm
Yes
Is there a high risk to rights and freedoms?
Yes
Use the evaluation doc
No
Record incident with any actions and improvements
Use the Incident Report Form
Notify SMT and Coms immediately
Notify IC within 72 hours
Implement recovery plan to minimise risks
Co-operate with IC investigation
Yes
Serious ? Notify affected data subjects
Notify all individuals concerns as soon as possible - log coms
Identify lessons learned and apply cross college
Report to SMT / Governors

9. Disciplinary

9.1 For College Group employees' failure to follow the correct procedure or ignoring a possible data breach may result in disciplinary action.

10. Review

10.1 The policy and procedure will be reviewed in line with legislation changes, case law or no later than two years after the issue date.

Appendix 1 Data Breach Incident Report Form

This form is also located on Data Protection SharePoint page.

Description of the data breach	
Date and time breach was identified	
Name of the person who identified the breach	
Name of the person reporting the breach	
Contact details Telephone/Email	
Classification of data breached **a. Public** **b. Internal** **c. Confidential** **d. Protected**	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or on-going?	
If on-going, what actions are being taken to recover the data?	
Who has been informed of the breach?	
Evaluation of incident severity	
Any other relevant information	

Email this form to: dpo@ucscollegegroup.ac.uk

Received by	
Date/Time	

Appendix 2 Data Breach Checklist

Step	Action	Notes
A	**Containment and recovery**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data**
1	Data Protection Officer to ascertain the severity of the breach and determine if any personal data is involved	Use the Evaluation of Incident Severity
2	Data Protection Officer to forward Data Breach Incident Report Form to Principal	To oversee full investigation and produce report. If personal data has been breached contact the IC as appropriate.
3	Identify the cause of the breach and whether it has been contained Ensure that the possibility of any further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all cross-College Group teams who can assist in this process. This may involve actions such as taking systems off-line or restricting access to systems to a limited number of staff until more is known about the incident.
4	Determine whether anything can be done to recover any losses and limit any damage that may be caused	Such as physical recovery of data/equipment or where corrupted through use of back-ups.
5	Where appropriate, the DPO to inform the police	Such as in the case of stolen property, fraudulent activity, offence under the Computer Misuse Act
6	Ensure all key actions and decisions are logged and recorded on the timeline	
B	**Assessment of Risk**	**To identify and assess the on-going risks that may be associated with the breach**
7	What type and volume of data is involved?	Data classification/volume of individual data etc.
8	How sensitive is the data?	Sensitive personal data?
9	What has happened to the data?	For example if the data has been stolen, it could be used for purposes which are harmful to the individuals to whom it relates; if damaged this poses a different type and level of risk
10	If the data was lost/stolen, were there any measures in place to prevent access/misuse?	For example encryption of the data or device

11	If the data was damaged/corrupted/lost, were there	For example being part of a back-up strategy
12	How many individuals' are affected?	Consider when/how to give notice
13	Who are the individuals whose data has been compromised?	Students, applicants, staff, customers, suppliers, employers
14	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data
15	Is there actual/potential harm that could come to any individuals?	For example are the risk to: Physical safety Emotional wellbeing Reputation Finances Identity Or a combination of these and other private aspects of their lives
16	Are there any wider consequences to consider?	If there a risk to public health or loss of public confidence in the College Group?
17	Are there others who should be made aware of the incident because of risks / courses of action?	For example if bank account details have been lost, consider contacting the banks themselves for advice on anything they can do to help prevent fraudulent use
C	**Consideration of Further Notification**	**Notification if to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions**
18	Are there any legal, contractual or regulatory requirements to notify?	For example terms of funding, contractual obligations
19	Can notification help the College Group meet it's security obligations under the UK GDPR?	Prevent any unauthorised access, use or damage to the data or loss of it.
20	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing their password or monitoring their account)?
21	If a large number of people are affected or there are very serious consequences, inform the IC	
22	Consider the dangers of 'over notifying'	Notify only when necessary – be practical about notifications.
23	Consider who needs to be notified, what you will tell them and how this will be communicated	Always consider the security of the medium of communication as well as the urgency. Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach.

		Give specific and clear advice to individuals on the steps they can take to protect themselves and how the College Group can help them. Provide a way for them to contact us for further information or to ask questions about what has happened (e.g. a contact name, helpline number or a web page).
24	Consult the IC guidance on when and how to notify it about breaches	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the IC where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases should be considered on their own merit and there is no precise definition of what constitutes a large volume of personal data.
25	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals	e.g. police, insurers, professional bodies, trade unions, website/system providers, bank/credit card companies.
D	**Evaluation and Response**	**To evaluate the effectiveness of the College Groups response to the breach**
26	Establish where any present or future risks lie	How does this incident inform the development Group's business continuity policy?
27	Consider the data and contexts involved	What data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
28	Consider and identify any weak points in existing security measures and procedures. Do DPIAs and risk mitigation actions need updating?	In relation to methods of storage and/or transmission, use of storage devices, levels of access, system/network protection.
29	Consider and identify any weak points in levels of security awareness/training	Fill in any gaps through training or specific advice.
30	Report on findings and implement recommendations	Report to SMT/Governors.

Appendix 3 Timeline of Incident Management

Date	Time	Activity	Decision	Authorised by