Data Breach Policy and Procedure

This policy and procedure applies to all staff, learners, partners, governors, employers, suppliers or third parties we work with. It should be read in conjunction with the colleges Data Protection Policy https://www.hull-college.ac.uk/the-college/data-protection-gdpr

The objective of this policy is to enable staff to act promptly to contain any breaches that occur, minimising the risk associated with the breach and to take action if necessary to secure personal data and prevent further breaches.

The college expects its staff to embed security and prevention practices in their normal working day to ensure personal, or special category, data is protected for the purposes of college business and must take appropriate steps to safeguard this information.

What is a data breach?

A personal data breach is 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 in connection with the purposes of the colleges business.

A breach in IT security or an external threat to college networks or systems should also be documented and investigated in the same way.

A personal data breach includes, but is not restricted to, the following:

- Loss or theft of data or equipment on which personal or sensitive data is stored (i.e. loss of laptop, USB pen, iPad/Tablet device, or paper record)
- Inappropriate access controls allowing unauthorised use
- Equipment theft or failure
- Unforeseen circumstances such as fire or flood
- Hacking attack
- Human error
- Offences where information is obtained by deceiving the holder of the information, the college
- Unauthorised disclosure of sensitive/personal data

Destruction of paperwork or electronic records in accordance with the internal Retention and Destruction Policy does not constitute a breach.

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 **John Applegate** and any breach, or suspected breach, can be sent for his attention on GDPR-Breach@hull-college.ac.uk

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

False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable the college 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 breach, even if you are unsure whether or not it is a breach.

BECOMING AWARE OF A DATA BREACH – INVESTIGATING

We become aware of a 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's Office (ICO)** will commence.

When you report a data breach to the college 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, 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 ICO data breach may result in disciplinary action.

ASSESSING A DATA BREACH

Once you have reported a breach and our 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, our DPO will notify management. If necessary, we 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 and any individuals affected.

If our 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

Our 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, our 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 INFORMATION COMMISSIONER'S OFFICE (ICO)

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 ICO 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 our DPO, and any notification to the ICO 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 ICO 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. Our 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 ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, our DPO will consider whether we need to update the ICO about the data breach.

EVALUATION AND RESPONSE

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

It is extremely important to identify the actions that the College 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 procedures to minimise the likelihood of incidents occurring again.