Bury College Data Breach Notification Procedure

Contents

Bury College Data Breach Notification Procedure

Where there is a medium to high level data breach within the College, it is a legal requirement to notify the ICO within 72 hours and the individuals concerned as soon as possible. It is essential therefore that all data breaches, no matter how big or small, are reported to the Data Protection Officer (DPO).

This Procedure should be read in conjunction with our Data Protection Policy, Data Retention Policy, and Privacy Policy. Our Data Protection Policy contains information on what constitutes a data breach and under what circumstances they should be reported to the Information Commissioner's Office (ICO); please read it to make sure that you aware of the breadth of what could be considered a data breach.

This Procedure should be followed by all staff. At all stages of this procedure, our DPO and management will decide whether to seek legal advice. This procedure will also apply where we are notified by any third parties that process personal data on our behalf, or any organisation that we share information with under an information sharing agreement, that they have had a data breach which affects our personal data.

The ICO can issue penalties for severe data breaches against organisations. Details can be found at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/

The procedure is set out below. Any failure to follow this procedure may result in disciplinary action.

IDENTIFYING AND REPORTING A DATA BREACH

If you discover a data breach, ; you must report this to our DPO immediately. The Data Protection Officer can be contacted at dpo@burycollege.ac.uk . Any other questions about the operation of this procedure or any concerns that the procedure has not beenfollowed should be referred in the first instance to the Data Protection Officer.

A data breach could be as simple as putting a letter in the wrong envelope and therefore even the most minor data breaches ***must*** be reported. If a data breach is reported a Bury College, a data breach form will need to be completed and sent to the DPO for action.

Near misses or breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable us to learn lessons in how we respond, can help us strengthen processes to stop data breaches happening in the future, and help us put remedial action in place.

We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you do 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 being compromised. From this point, our time limit for notification to the ICO will commence.

When you report a data breach to our Data Protection Officer, they will promptly investigate the breach to ascertain whether we are fully aware that are breach has occurred that has led to personal data being compromised.

WE WILL AIM TO DO THIS BY CLOSE OF PLAY THE FOLLOWING WORKING DAY OF A BREACH BEING REPORTED TO US.

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, the DPO will log the breach in our Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity. If the breach has occurred within the DPOs management area they will consult the Director of HR, and the Vice Principle of Finance and Corporate Resources, to confirm the severity and whether the ICO needs to be notified. This is to avoid any conflict of interest between the role of DPO and their management role within the College.

Once the level of severity is known, our Data Protection Officer 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 of high impact, they will consider the impact on our reputation and the effect it may have on the trust placed in us. Our DPO and senior management will consider whether to appoint a PR professional to advise on reputational damage and will also consider whether legal advice is needed.

WE WILL AIM TO DO THIS BY CLOSE OF PLAY THE FOLLOWING WORKING DAY OF US BECOMING AWARE OF THE BREACH.

FORMULATING A RECOVERY PLAN

Our DPO and senior management will investigate the breach and consider a recovery plan 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.

WE WILL AIM TO DO THIS BY CLOSE OF PLAY THE FOLLOWING WORKING DAY OF ASSESSING THE BREACH.

NOTIFYING A DATA BREACH TO THE ICO

Unless the breach considered to be of low detriment 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.

The content of the notification will be drafted by our DPO in line with our Data Protection Policy, and the notification will be made by our Data Protection Officer – please be aware that **under no circumstances must you try and deal with a data breach yourself**.

THIS WILL BE DONE WITHIN 72 HOURS OF BECOMING AWARE OF THE BREACH.

NOTIFYING A DATA BREACH TO INDIVIDUALS

We must also notify the individuals concerned as soon as possible.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Protection Policy 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, explained in our Data Protection Policy, we may not need to notify the affect individuals. Our DPO will decide whether this is the case.

THIS WILL BE DONE AS SOON AS POSSIBLE AFTER WE BECOME AWARE OF THE BREACH, IDEALLY WITHIN 72 HOURS.

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 management. They will decide on the content of such notifications.

WE WILL AIM TO DO THIS WITHIN FIVE DAYS OF BECOMING AWARE OF A DATA BREACH.

CONSIDER WHETHER NOTIFICATIONS NEED TO BE UPDATED

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.

THIS WILL BE CONSIDERED ON AN ONGOING BASIS.

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 management will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register.

]