Wirral Met College

*1Wirral Met Logo*

# Data Breach Notification Procedure

| | |
|---|---|
| Document status | |
| Document owner | Assistant Principal MIS |
| Document author | Assistant Principal MIS |
| Document type | Process |
| Date of document | November 2023 |
| Version number | 06 |
| Review requirements | Annual |
| Date of next review | November 2024 |
| Approval body | SLT |
| Publication | Staff Intranet / Website |
| Code | PS34 |

# Data Breach Notification Procedure

Where there is a data breach as defined by the Information Commissioners Office (ICO) within the College, it is a legal requirement to notify the ICO within 72 hours.

It is not required that staff make the decision whether or not a data breach has occurred. The decision and appropriate actions will be agreed by the Data Protection Officer in conjunction with Senior Leadership and management team members and where appropriate external advice.

This Procedure should be read in conjunction with our Data Breach Policy and Data Protection Policy.

This procedure will also apply where we are notified by any third parties that process personal data on our behalf that they have had a data breach which affects our personal data.

## IDENTIFYING AND REPORTING A DATA BREACH

If you discover a data breach, however big or small, you must report this to our Data Protection Officer immediately. The Data Protection Officer is Paul Groome – Assistant Principal, MIS. Any other questions about the operation of this procedure or any concerns that the procedure has not been followed should be referred in the first instance to the Data Protection Officer.

A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches ***must*** be reported.

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 AND NOTIFYING ICO

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, our Data Protection Officer 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.

The Data Protection Officer will assess if the breach may be reportable and contact the ICO for advice and/or to report the incident

**THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED**

## ASSESSING A DATA BREACH

Once you have reported a breach and our Data Protection Officer has investigated a decision will be made if a reportable breach has occurred. If so, the Data Protection Officer will log the breach in our Data Breach Register and notify the Information Commissioners Office.

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.

**THIS WILL BE DONE WITHIN 72 HOURS OF THE BREACH OCCURING**

## FORMULATING A RECOVERY PLAN

Our Data Protection Officer will investigate the breach and agree a recovery plan to minimise the risk to individuals. As part of the recovery plan, our Data Protection Officer 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 INDIVIDUALS

Where a breach is notifiable to the ICO 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. In some circumstances we may not need to notify the affect individuals. Our Data Protection Officer will decide whether this is the case.

The content of the notification will be drafted 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 AS SOON AS POSSIBLE AFTER WE BECOME AWARE OF THE BREACH.**

## 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 Data Protection Officer and management. They will decide on the content and timeline for such notifications.

## 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 Data Protection Officer 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.

Following all reportable incidents a review of the breach will take place and lessons learned and actions taken reported to the Executive management team.