HIGH SPEED RAIL

The National College

National College for High Speed Rail
DATA BREACH NOTIFICATION PROCEDURE

Document Reference	NCHSR-GDPR-DBNProcedure
Version	FINAL
Author	Sally Brook Shanahan
Owner	Sally Brook Shanahan - DPO
Workstream / Business area	GDPR Working-Group
Classification	Public
Approval Level	SMT
Version approval date	23rd May 2018 - SMT
Review schedule	Annually
Next review date	May 2019

DATA BREACH NOTIFICATION PROCEDURE

Where there is a 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 in certain situations. It is essential therefore that all data breaches, no matter how big or small, are reported to us.

This Procedure should be read in conjunction with our Data Breach Policy and Data Protection Policy. Our Data Breach Policy contains detailed information on what constitutes a data breach; please read it to make sure that you aware of the breadth of the concept of a data breach.

This Procedure should be followed by all staff. At all stages of this procedure, our Data Protection Officer 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 that they have had a data breach which affects our personal data.

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, however big or small, you must report this to our Data Protection Officer immediately. The Data Protection Officer is Sally Brook Shanahan and can be contacted at: dataprotectionofficer@nchsr.ac.uk 0121 295 6754 or 07920 450641. 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 placing a letter being in the wrong envelope and therefore even the most minor data breaches ***must*** be 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 us to learn lessons in how we respond and the remedial action we put 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, 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.

THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.

ASSESSING A DATA BREACH

Once you have reported a breach and our Data Protection Officer has investigated it and has decided that we are aware that a breach has occurred, our Data Protection Officer 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 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 Data Protection Officer 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. Our Data Protection Officer and senior management will consider whether it is necessary to appoint an external PR professional to advise on reputational damage and will also consider whether external legal advice is needed.

THIS WILL BE DONE WITHIN 24 HOURS OF US BECOMING AWARE OF THE BREACH.

FORMULATING A RECOVERY PLAN

Our Data Protection Officer 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 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.

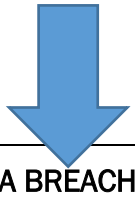
THIS WILL BE DONE WITHIN 24 HOURS OF ASSESSING THE BREACH.

NOTIFYING A DATA BREACH TO THE ICO

Unless the breach is unlikely to 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 Data Protection Officer in line with our Data Breach Notification 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 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 Data Protection Officer in line with our Data Breach Notification 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 Breach Notification Policy, we may not need to notify the affect individuals. Our Data Protection Officer will decide whether this is the case.

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 of such notifications.

THIS WILL BE DONE WITHIN 5 WORKING 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 Data Protection Officer 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 Data Protection Officer 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.