Nescot

Personal Data Breach Policy and Notification Procedure

College Personal Data Breach Policy and Notification Procedure

Personal Data Breach Notification Procedure

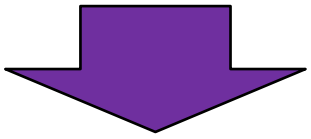
Business Requirement

Where there is a personal data breach within the College, it is a legal requirement **to notify the Information Commissioners Officer (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 the Data Breach Policy also contained within this document. 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 Susanne Wicks and can be contacted at: dataprotection@nescot.ac.uk.
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.
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.

Should the Data Protection Officer be on away from the College on leave then the role of investigation and reporting of the breach is delegated to the Duty Manager

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 the impact on reputational damage and will also consider whether 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 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 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 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

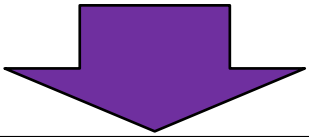
The decision as to whether any third parties need to be notified will be made by our Data Protection Officer and management. They will decide on the content of such notifications.

THIS WILL BE DONE WITHIN 5 DAYS OF BECOMING AWARE OF A DATA BREACH.

CONSIDER WHETHER NOTIFICATION NEEDS 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.



CONSIDER WHETHER NOTIFICATION NEEDS TO BE UPDATED

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.

Personal Data Breach Policy

1. OVERVIEW

The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. As an organisation that collects and uses Personal Data, the College takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise. The College's key concern in relation to any breach affecting Personal Data is to contain the breach and take appropriate action to minimise, as far as possible, any adverse impact on any individual affected. The College has therefore implemented this Policy to ensure all College Personnel are aware of what a Personal Data reach is and how they should deal with it if it arises.

College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College Personnel are obliged to comply with this Policy at all times.

2. ABOUT THIS POLICY

This Policy explains how the College complies with its obligations to recognise and deal with Personal Data breaches and (where necessary) to notify the ICO and the affected individuals. The College has a corresponding Data Breach Notification Procedure and Data Breach Register that set out how the College deals with and records Personal Data breaches.

3. SCOPE

This Policy applies to all College Personnel who collect and/or use Personal Data relating to individuals. It applies to all Personal Data stored electronically, in paper form, or otherwise.

4. DEFINITIONS

4.1. **College** – North East Surrey College of Technology (Nescot)

4.2. **College Personnel** – Any College employee or contractor who has been authorised to access any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

4.3. **Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

4.4. **Data Protection Officer** – The Data Protection Officer is Susanne Wicks and can be contacted at: 0208 394 3004, dataprotection@nescot.ac.uk.

4.5. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

4.6. **Personal Data** – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

4.7. **Special Categories of Personal Data -** Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

5. WHAT IS A PERSONAL DATA BREACH

5.1. The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

5.2. Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

5.3. A Personal Data breach could include any of the following:

5.3.1. loss or theft of Personal Data or equipment that stores Personal Data;

5.3.2. loss or theft of Personal Data or equipment that stores the College's Personal Data from a College supplier;

5.3.3. inappropriate access controls meaning unauthorised College Personnel can access Personal Data;

5.3.4. any other unauthorised use of or access to Personal Data;

5.3.5. deleting Personal Data in error;

5.3.6. human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing Personal Data on a train);

5.3.7. hacking attack;

5.3.8. infection by ransom ware or any other intrusion on our systems/network;

5.3.9. 'blagging' offences where information is obtained by deceiving the organisation who holds it; or

5.3.10. destruction or damage to the integrity or accuracy of Personal Data.

5.4. A Personal Data breach can also include:

5.4.1. equipment or system failure that causes Personal Data to be temporarily unavailable;

5.4.2. unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;

5.4.3. inability to restore access to Personal Data, either on a temporary or permanent basis; or

5.4.4. loss of a decryption key where Personal Data has been encrypted because this means the College cannot restore access to the Personal Data.

6. REPORTING A PERSONAL DATA BREACH

6.1. College Personnel must immediately notify any Personal Data breach to the Data Protection Officer, no matter how big or small and whether or not College Personnel think a breach has occurred or is likely to occur. This allows the College to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the College.

6.2. If College Personnel discover a Personal Data breach outside working hours, College Personnel must notify it to the College's Data Protection Officer as soon as possible.

6.3. College Personnel may be notified by a third party (e.g. a supplier that processes Personal Data on the College's behalf) that they have had a breach that affects College Personal Data. College Personnel must notify this breach to the College's Data Protection Officer and the College's Data Breach Notification Procedure shall apply to the breach.

7. MANAGING A PERSONAL DATA BREACH

7.1. There are four elements to managing a Personal Data breach or a potential one and this Policy considers each of these elements:

7.1.1. Containment and recovery

7.1.2. Assessment of on-going risk

7.1.3. Notification

7.1.4. Evaluation and response

7.2. At all stages of this Policy, the Data Protection Officer and managers will consider whether to seek external legal advice.

8. CONTAINMENT AND RECOVERY

8.1. An initial assessment of the Personal Data breach will be carried out by the Data Protection Officer.

8.2. If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected then it will be added to the College's Data Breach Register and no further action will be taken.

8.3. If the Personal Data breach may impact on the rights and freedoms of the individuals affected then the College will put together and implement a bespoke Personal Data breach plan to address the breach concerned in accordance with the College's Data Breach Notification Procedure. This will include consideration of:

8.3.1. whether there are any other people within the College who should be informed of the breach, such as IT team members, to ensure that the breach is contained;

8.3.2. what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and

8.3.3. whether it is necessary to contact other third parties such as students, parents, banks, the ICO or the police particularly in the case of stolen Personal Data. All notifications shall be made by the Data Protection Officer.

8.4. All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Officer.

8.5. The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

9. ASSESSMENT OF ONGOING RISK

As part of the College's response to a Personal Data breach, once the breach has been contained the College will consider the on-going risks to the College and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with the College's Data Breach Notification Procedure.

10. NOTIFICATION

10.1. Under Data Protection Laws, the College *may* have to notify the ICO and also possibly the individuals affected about the Personal Data breach.

10.2. Any notification will be made by the Data Protection Officer following the College's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

10.3. Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within **72 hours of** when the College becomes aware of the breach unless it is *unlikely to result in a risk to the rights and freedoms of individuals* . It is therefore imperative that College Personnel notify all Personal Data breaches to the College in accordance with the Data Breach Notification Procedure immediately.

10.4. Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is *likely to result in a high risk to the rights and freedoms of individuals.*

10.5. Please note that not all Personal Data breaches are notifiable to the ICO and/or the individuals affected and the College will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

10.6. Where the Personal Data breach relates to a temporary loss of availability of the College's systems, the College does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of individuals. The College does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case-by-case basis in accordance with the Data Breach Notification Procedure.

10.7. In the case of complex breaches, the College may need to carry out in-depth investigations. In these circumstances, the College will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

10.8. Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the Personal Data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

10.9. When the College notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be done in accordance with the Data Breach Notification Procedure. Any notification to an individual should include details of the action the College has taken in relation to containing the breach and protecting the individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

10.10 The College may not be required to notify the affected individuals in certain circumstances as exemptions apply. Any decision whether to notify the individuals shall be done in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Officer.

11. EVALUATION AND RESPONSE

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

11.2. There will be an evaluation after any breach of the causes of the breach and the effectiveness of the College's response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Personal Data Breach Register.

11.3. Any remedial action such as changes to the College's systems, policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

Personal Data Breach Policy and Notification Procedure

VERSION	3
Policy Originator	Data Protection Officer
Equality Impact Assessed:	
Approved by:	SMT
Date Approved:	June 2018
Review Interval:	3 years
Last Review Date:	Aug 2023
Next Review Date:	Aug 2026
Audience:	Public

Nescot