Personal Data Breach – Identification and action

The decision to report a data breach, either to the Information Commissioners Office (ICO) or to the data subjects themselves, remains solely with the Group's Data Protection Officer (DPO).

It is the duty of all Group staff to report data breaches to the DPO (via the dp@rnngroup.ac.uk email address) as soon as they become 'aware' of a breach. Awareness is defined as when a member of staff has a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised.

Sanctions can be applicable to the Group should we fail in our obligations under the General Data Protection Regulations (GDPR) to report a data breach to the ICO, these could potentially be damaging to our reputation.

The GDPR explains that a personal data breach can be categorised as:

"Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data

"Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data

"Integrity breach" - where there is an unauthorised or accidental alteration of personal data

It should also be noted that, depending on the circumstances, a breach could concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

You will find below some fictional examples to aid you in identifying data breaches, the notification process that the DPO follows and additional information relating to the scenario presented.

Example	DPO to notify supervisory authority (ICO)?	DPO to notify the data subject?	Comments
Personal data is on an encrypted USB stick. The USB stick is stolen during a break in.	No.	No.	As long as the data is encrypted with a 'state of the art algorithm' (throughout the RNN Group, this is encryption to AES256 standards for providing personal information) and the unique key is not compromised, this is not a reportable breach.
Personal data is removed from a secure web site managed by the Group during a cyber-attack.	Yes. DPO will report to the ICO and will identify if there are any potential consequences to individuals.	Yes. DPO will inform individuals depending on the nature of the personal data affected and the potential consequences to them.	Even if the risk is deemed as 'not high' to individuals, the DPO may still opt to inform the data subjects of the breach as this initial disclosure may result in additional confidentiality breaches elsewhere.

A brief power outage lasting several minutes at a Group site means learners and staff cannot access their records.	No.	No.	This is not a notifiable personal data breach, it should however be recorded as an incident by the data protection team on the Group's central records.
A ransomware attack takes place that results in data being encrypted. No backups are available and the data cannot be restored. After investigation, it becomes clear that only encryption took place and no other malware was present.	Yes.	Yes. Only the individuals affected need to be notified where there is positive, clear, affirmation that others remained unaffected.	If there was a backup available and data could be restored in good time then this would not need to be reported, as there would be no permanent loss. However, the ICO may consider an investigation to assess compliance in a broader sense. It should however be recorded as an incident by the data protection team on the Group's central records.
An individual has received communication from the Group containing personal data of someone else. Within the initial 24 hour investigation, it becomes clear that a personal data breach has occurred and that other individuals may be affected.	Yes.	Yes. Only the individuals affected need to be notified where there is positive, clear, affirmation that others remained unaffected.	If after further investigation, it is found that more individuals are affected then the DPO shall update the ICO accordingly. The DPO may, in certain circumstances, have to notify other individuals if the level of risk to them has increased following the investigation.
A cyber-attack occurs where usernames, passwords and other personal details are published online by the attacker.	Yes.	Yes. This is defined as high risk to the individuals themselves.	Password resets should be enforced on the affected accounts with a view to extend this to all users should the risk be determined as possible. Other steps must be employed to mitigate the risk to the affected individuals wherever possible.
A website hosting company for the Group identifies an error in the code that controls user authentication. The effect means that any user can access any account details.	Yes. The website hosting company must notify its affected clients without undue delay. The website company must inform the Group of the data breach and the actions already taken. It is then the Group's responsibility to inform the ICO of the data breach.	Yes. By both the website hosting company (where applicable) and the Group themselves, where the risk is determined as high.	In this instance, the website hosting company is a processor for the Group (as controller), they have a responsibility to the data subject to inform them of the breach and this responsibility would already have been detailed to them in the 3rd party data processing agreement with the Group. The Group also has a responsibility to inform the individuals as it may cause reputational damage.

Occupational Health records are not available for a period of 30 hours due to a cyber-attack.	Yes. This potentially could be a high risk to the data subject's well-being and breach of privacy may occur.	Yes. DPO will inform individuals (depending on the nature of the personal data affected) and the potential consequences to them.	Occupational Health records are classed as special categories of data and a different lawful basis (explicit consent) must be employed for the data collection itself and any other processing.
Personal data of 5,000 students are mistakenly sent to the wrong mailing list with 1,000+ recipients.	Yes.	Yes. DPO will inform individuals depending on the scope and type of personal data involved and the severity of possible consequences.	This would be classed as reckless handling of data, all efforts would need to be employed to mitigate further risks to the rights and freedoms of the data subjects themselves.
A direct marketing email is sent to recipients in the 'to' field rather than the 'bcc' field thereby enabling each recipient to see the email address of other recipients.	Yes. Further action may be needed if a large number of data subjects are affected, special categories of data disclosed or another high risk is identified e.g. usernames and passwords.	Yes. DPO will inform individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification to the data subjects may, in certain circumstances, not be necessary e.g., if no special categories of data are disclosed or if the numbers affected remain low. Circumstances may change as the investigation progresses, the option to inform the data subjects may also have to be reviewed later in the investigation.