Reporting a data breach

What is a personal data breach?
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor; Sending personal data to an incorrect recipient, computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and loss of availability of personal data.
- Unforeseen circumstances like a fire, hacking or flood.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.
- A data processor may have suffered a data breach e.g SIMs which in turn effects the school.

However the breach has occurred, there are four important elements to any breach management plan:

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response
-

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it.

Breach reporting
If you are unable to log onto the GDPRis portal to report your data breach (see breach reporting procedure for further information on this) please complete the form below and email it to your schools DPO.

Data Protection Breach Reporting Form

Please provide as much information as you can at this stage. Your initial response should be provided **within 12 hours**. Do not delay returning the form if you do not know the answers to all questions. Please provide the information you know at present and follow up with additional information if further detail becomes available. Forms should be sent to skotb@koinoniafederation.com .

Contact information

Person making the report Name: Email:
Member of SLT you have informed: Name: Email:
Data Protection Officer Name: Sarah Kotb Email: Skotb@koinoniafederation.com
Organisation (data controller) school name:
Organisation registered address:

Breach information

Report Type • Initial report☐ • Follow up ☐
When did you discover the breach? Date: Time: When did the breach actually happen? Date: Time:
Please explained what happened and how the incident took place.
If there has been a delay in reporting the incident please explain the reasons for this.
What measures were in place to prevent an incident of this nature occurring?

Personal data placed at risk

What personal data has been placed at risk? Please specify if any financial or sensitive personal data (special categories) has been affected and provide details of the extent. Special Categories of Personal data include: • The racial or ethnic origin of the data subject ☐ • Their political opinions ☐ • Their religious or philosophical beliefs ☐ • Whether they are a member of a trade union ☐ • Their genetic data ☐

- Biometric data used to uniquely identify them ☐
- Their physical or mental health or condition ☐
- Their sex life or sexual orientation ☐

Please explain further

How many individuals have been affected and how many data records are involved?

Number of individuals (data subjects):

Number of personal data records:

Category of data subject affected.

- Employee ☐
- Users ☐
- Students ☐
- Not yet known ☐
- Other (please explain) ☐

What is the likely hood data subjects will experience significant consequences as a result of the breach?

- Very likely ☐
- Likely ☐
- Neutral ☐
- Unlikely ☐
- Very unlikely ☐
- Not yet known ☐
- Other (please explain) ☐

Are the data subjects involved aware of the incident and have any complaints been made?

(Cyber incident only) Has the confidentiality, integrity or availability of your information system been affected?

- Yes ☐
- No ☐
- Don't know ☐

(Cyber incident only) Impact on your organisation.

- High- Lost the ability to provide all critical services ☐
- Medium- Have lost ability to provide critical services to some users ☐
- Low- No loss of efficiency, service still available ☐
- Not yet known ☐

Containment and recovery (If unable to complete the DPO will fill this out)

Has any action been taken to minimise/mitigate the effect on the affected individuals? If so, please provide details.
Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
What steps have been taken to prevent a recurrence of this incident?
(Cyber incident only) Recovery time. • Regular- You can predict your recovery time with existing resources ☐ • Supplemented- You can predict your recovery time with additional resources ☐ • Extended- You cannot predict your recovery time and need extra resources ☐ • Not recoverable- recovery from incident is not possible e.g. Backups can't be restored ☐

Miscellaneous

Have the police or any other regulatory bodies been informed about this incident?
Has there been any media coverage of the incident?
Has the member of staff involved in this breach received data protection training in the last two years? • Yes ☐ • No ☐ • Don't know ☐

Further actions (To be completed by DPO)

What further actions have been taken in relation to this incident?
Will the breach be reported to the ICO?
Will the incident be reported within the 72 Hour time frame? Please explain any delays?