Data breach guide

What is a data breach:

A data breach is a breach of security leading to the accidental or unlawful loss, destruction, alteration, access to, or disclosure of, personal data.

Step 1 - Identifying a data breach:

It is important to be able to identify a data breach or a near miss as action will need to be taken and measures will need to be implemented to avoid further breaches occurring in the future.

To assist you with identifying a data breach, we have set out some common examples below:

- Sending an email containing any personal information to the incorrect recipient;
- Sending a letter containing any personal information to the incorrect recipient;
- Leaving laptops or computers unlocked and unattended;
- Sharing passwords with others;
- Writing passwords down, especially where these are left unattended or with the device that the password applies to;
- Leaving personal information lying around where others (especially non-staff members) can access/see that information; or
- Phishing emails – clicking on links in emails when you are unsure of the sender or validity of the email;

This is not an exhaustive list and there may be other incidents that amount to a data breach. If you are in doubt, use your DPOCOMS dashboard to report the breach and your DPO will be able to advise you.

Step 2 – report the breach to your DPO:

Use the DPOCOMS dashboard 'report a data breach' function to log the data breach with your DPO. You should also use this to log any near misses that you encounter.

To complete this initial report to your DPO you will need to provide the following information:

- Date the breach was discovered – this may be different from the date the breach occurred. It is important for the DPO to know the date the breach was first discovered as this is the date from which the 72 hours to report is calculated.

- Nature of the breach – you should contain basic information about the nature of breach or what has happened that has resulted in a breach, e.g. lost memory stick, not protected by password.
- Details of the breach – this should set out information about what type of personal data has been compromised because of the breach. For example, the memory stick contained the full names, DOB, address and exam results information for all students in year 11.
- Any action taken on discovering the breach – you should list any actions/steps taken following discovery of the breach, e.g. a full search of the school was carried out for the memory stick.
- Personal information compromised – you should upload any files containing personal information that are relevant to the breach.

Once you have provided this initial information, your DPO may request further information and it may be necessary to complete a full data breach report form. Your DPO may do this once they have gathered all the necessary information, or you may be asked to do this with guidance from your DPO.

Step 3 – contain the breach:

Whilst this appears as step 3 in this guide, you should take any steps to contain the breach as soon as you discover the breach. Usually, you will be required to act quickly, reporting the breach to the DPO and containing the breach should happen at the same time or one straight after the other.

It may be that you need assistance from your DPO, IT manager or other professional (e.g. the police or cyber security specialists) to contain the breach. Please seek advice from your DPO if you are unsure about who may assist with containing the breach.

Please note that some steps that you could take to contain the breach may include – securing your network, changing passwords or retrieving data/emails (where possible).

Containing the breach may take several different measures and could take some time. You will need to make this a priority. If it becomes apparent that the breach will need to be reported to the Information Commissioner's Office ('ICO'), where possible, you should do this as you are implementing the measures to contain the breach.

Step 4 – investigate the breach:

Your DPO will lead in investigating the circumstances surrounding the data breach and any consequences of the breach. They will require the assistance of key personnel in your school/academy to complete the breach investigation. They will need to speak to, or receive information from, any staff involved in the breach.

Please ensure you are available for the DPO to speak to regarding the breach.

Depending on the nature of the breach, the investigation may take some time.

At the earliest opportunity in the investigation, your DPO will assess whether it is necessary to report the breach to the ICO. If a report to the ICO is required, it doesn't mean the investigation will cease pending a response. The investigation will continue and the DPO may need to update the ICO following the initial report, even if they have not yet received a response.

Step 5 – report the breach:

Your DPO will be able to assess whether the breach meets the threshold for reporting to the ICO and would make that report on your behalf.

It is important to act quickly when a breach is discovered as we have 72 hours from the time of discovering the breach to report it to the ICO. If we report the breach outside this timescale, we will need to provide information about why the report was delayed.

The ICO have a report form that will need to be completed and submitted online, this form asks for the following information:

- Name and details of your school;
- Name and details of your DPO;
- Details of how the breach occurred;
- Details of the personal information involved in the breach;
- Additional questions if it is a cyber security breach;
- Details of any steps taken to contain the breach;
- Details of any steps to mitigate the risk of the breach occurring again in the future; and
- Information regarding any data protection training that the individuals involved have received.

There are further questions covered by the report form, but these are the main question areas.

Once your DPO has reported the breach, they will receive a response with a case reference number that will need to be quoted, should they need to submit any further information whilst the ICO are considering the information.

It can take some time to hear back from the ICO following the submission of a data breach report form. You should continue to investigate and take any necessary measures to contain and mitigate the risk in the meantime.

Step 6 – conclude the investigation:

Your DPO will continue to investigate the breach and may advise of further steps required to contain the breach.

You may also need to notify the data subjects who have been impacted by the data breach and/or submit a press release regarding the breach.

Your DPO will be able to advise you on this and work with you to release the appropriate information to data subjects/the public at the relevant time.

It may be necessary for your DPO to provide further information to the ICO during this stage.

Once the investigation is complete, the DPO will breach a report and may provide you with a breach outcome investigation letter to provide to any impacted data subjects.

The investigation may conclude before hearing back from the ICO. It may be necessary to reopen the investigation if further questions are flagged up by the ICO.

Step 7 – mitigate the risk:

This is the part of the process where you take action to try and reduce the risk of this type of breach occurring again in the future. You may already have implemented some measures but at this point your DPO will review all required measures and advise you of these.

The type of measure required will depend on the type of breach that has occurred, but some examples include:

- Specific data protection training
- Implementation of a new policy or process
- Purchase of security software

This is not an exhaustive list.

Mitigating the risk is about demonstrating that you have learnt from the mistakes that resulted in the current breach and are actively taking measures to ensure that these mistakes do not happen again.

Record Keeping:

It is important to keep a log of all data breaches and near misses that occur. DPOCOMS keeps this record for you with dates, details and any key actions of all breaches that you have encountered. You may require this information for audit purposes.

You should use these records to inform your data protection training plans.