# GUIDANCE NOTE – DATA BREACH REPORTING

This guidance note accompanies the document "Data Breach Report Form," designed to assist Schools in completing this form.

If you do have any questions about this document, please let us know.

## General

This is a standard document that can be used to report a data breach to the ICO in accordance with your breach notification policy.

You can also report breaches to the ICO by going onto the Jedu portal, clicking on the "breaches" tab and click "open new breach." Once you submit the portal form, this will be sent to Judicium to review before sending to the ICO.

## Legal Position

Under the UK GDPR, you must notify the ICO of breaches which result in a risk to the rights and freedoms of individuals. This report must be made within 72 hours and when reporting to them you must provide: -

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer as well as the contact within the school;
- a description of the consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

## Who Should Complete the Form?

This will normally be conducted by a staff member within the school who is either senior in the organisation (Headteacher, Business Manager) or the staff member responsible for reporting data breaches as set out within the policy. You should send this report to Judicium (your DPO) to review whether the breach is reportable to the ICO.

If you would like us to report any data breach, then please do email dataservices@judicium.com with plenty of time to enable us to make the report within 72 hours of the breach being made. We would suggest titling the email "URGENT DATA BREACH – ICO SUBMISSION REQUIRED BY DPO" and we can pick this up accordingly.

## How To Complete the Form?

We have set out below how to complete each section of the form. Please note that you may be unable to complete some sections in this form in detail because of the quick turnaround with the ICO. That is fine and additional details can follow later if you are unable to provide within 72 hours.

Summary Of the Breach

Detail the circumstances which have led to the breach including how you become aware of the breach, when the breach occurred and when you became aware of the breach.

Data Type and Individuals Affected

What information was affected and how many people are affected by the breach.

Try and add as much detail as possible including what documents were affected, what information was contained on those documents (for example date of birth, addresses), the categories (for example, parents, staff, children) and number of people affected.

You do not need to give names of individuals affected at this stage.

However, you can also detail any relevant circumstances about individuals which may escalate the breach (for example details of a child protection order, health issues).

Effects Of the Breach

This could be actual or potential effects (such as loss of confidentiality, breach of security). Detail the risk to the school as well as to the individuals affected and who has received (or could be in receipt of) the data.

Actions Taken

Detail here all actions taken to remedy the breach, including the actions taken by those who accidentally received the information and the actions the school have taken to remedy the breach. Has the breach been contained? If so, how was it contained.

Has the person who caused the breach been made aware, have the school spoken with them?

Also set dates that these actions have happened where possible.

It's also important to detail here whether the data subject has been notified yet and if not why (for example because we didn't foresee there was a high risk).

Data Protection Measures in Place

To benefit the ICO, set out here the measures in place (both generally and specific to this situation in question) to protect individual data. For example, detail policies in place such as data protection policy, any training that has taken place with staff, security measures to protect emails, password protection, authorised access, etc.).

This does not need to be detailed but helps the ICO understand what measures and processes you had in place to prevent this kind of incident from happening in the first place.

Any Other Relevant Information

To set out here any other relevant information to the breach. For example, any future actions you may be taking. Whether there is any further risk to the school of further breaches or affects taking place. If data has been transferred outside of the EU. If there have been previous matters with the ICO in the past.

You may also want to summarise here whether you feel the breach has now been contained.

Status

Finally, to inform the ICO if any further action is required by the school (i.e., whether further information is required to be provided to the ICO or not or if further investigation is required).

For example, if you have completed all investigation to say: -

We have conducted a review of this incident, details of which have been included in this form

If further action is still required to say: -

We are conducting a thorough review of this incident and aim to complete such review by September. We have included in the attachment to this letter as much relevant information as we have available at this time.