---

# Email

# ICO Decision ...

Regarding | Worked By | Statu

Activity Marker | Dire

## Email

**From** ICO Casework

**To** data.breach@bristol.gov.uk

**Cc**

**Subject** ICO Decision - IC-308626-H5K9

**Display Name**

**Date Received** 13/06/2024 16:30

**Email Address**

**13 June 2024**

**Reference Number IC-308626-H5K9**

**Dear** [redacted]

**I am writing further to your personal data breach report of 22 May 2024 regarding an child's EHCP which was emailed to another child's parents.**

**Thank you for the information you have provided.**

**Data security requirements**

**You are required to have appropriate technical and organisational measures in place to ensure the security of personal data.**

**Our Decision**

**We have considered the information you have provided and we have decided that no further action by the ICO is necessary on this occasion. This decision is based on the information we have recorded about the breach.**

**The reasons for our decision are as follows:**

**You advised that the incorrect recipient notified your organisation that they had received information relating to another individual. In addition, they have confirmed to you that the email has been permanently deleted and that they did not read the appendices attached. This may indicate that the breach is somewhat contained.**
**Preventative measures were in place as you advise staff undertake mandatory training, there is email encryption available for sharing sensitive documents and the service area receive specific training for dealing with EHCP's.**
**Steps are being taken to prevent a reoccurrence as the service area will ensure all mandatory training for the SEND team is up to date. You also advise a team meeting will be held to discuss the current process for distributing EHCP's and you will remind staff to double check information before issuing EHCP's to parents.**

**However, we recommend that you investigate the causes of this incident, to ensure that you understand how and why it occurred, and what steps you need to take to prevent it from happening again.**

**In particular, we recommend that you consider:**
**Continuing to handle the individual's complaint in line with your organisation's processes. Should any additional information become available which would impact the case please update us by quoting the above case reference number.**
**Seeking written confirmation from the incorrect recipient that they have retained no copies of the information and that it will not be shared or used further. This may provide you with additional assurances that the breach has been contained.**
**Ensuring that all relevant staff have completed the mandatory training. Where possible, data protection training should be refreshed annually or at a minimum every two years. This can help to maintain staff awareness regarding the correct processes to follow and may help to prevent data breaches.**
**Reviewing your organisation's processes for naming documents. If not already in place, ensure your document naming conventions are identifiable and consistent across the organisation to prevent documents from becoming mixed up. For example, blank forms could be labelled as 'Blank xxx – Master Copy' and checks should be carried out to ensure it**

**remains blank. Staff could be reminded not to store local copies and always get the blank master template from the relevant file on your system.**
**Password protecting documents containing more sensitive personal data. In addition, ensure that a unique password is used for each new document. This may help to prevent an incorrect recipient from accessing personal data in the event they are sent to an incorrect recipient.**
**Ensuring there are appropriate checking and verification measures in place with regards to sending personal data outside of your organisation. There should be a robust double-checking measure to ensure information is sent correctly. This includes checking recipient's details and any attachments as this may help to ensure the correct information is sent to the intended recipient.**
**Highlighting the importance of double-checking attachments and recipients when communicating both internally and externally. You could emphasise this within your data protection training for staff, and frequent reminders could be issued to ensure that data protection awareness remains embedded in daily tasks.**

**Please note that we may make additional enquiries if we become aware of new information which affects the circumstances of this case.**

**Please note that as a result of a breach an organisation may experience a higher volume of information rights requests and complaints, particularly in relation to access and erasure. If you receive these complaints, you should have a contingency plan, such as extra resources, to deal with them. You should not refer these complaints to the ICO as a matter of course, and it is important that you continue to deal with complaints, alongside the other work that has been generated as a result of the breach.**

**Thank you for reporting the incident. Further information and guidance relating to** data security **is available on our website.**

**We now consider the matter to be closed.**

**Yours sincerely**

**Rosina Harrison**
**Lead Case Officer**
**T. 03304146163**

## Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

## For information about what we do with personal data see our privacy notice.