Data Breach

Introduction

Data breach issues are a central concern of the new data protection regime. **Data can be both electronic and on paper.**

Pace has set up policies and procedures to limit data breaches, in as far as possible, e.g.:

- Virus software
- Cloud back up
- Locked storage of paper copies

However, as with all risks, it is not possible to insure against every eventuality as threats can come from a malicious virus, accidental loss, aggravated loss e.g. burglary, or fire etc.

If a member of staff of Pace becomes or is aware of a data breach it must be reported immediately to the Data Protection Lead (DPL) or, in their absence, to a member of the Leadership Team (Director of Finance & Operations, Director of Fundraising & Communications, Director of Education or Director of Clinical Services). The Head of IT should also be advised.

A data breach can include the loss of your personal smartphone or tablet, etc. on which you have the app that allows access to your work e mails and /or SharePoint.

The DPL will investigate the report and determine whether a breach has occurred and whether it requires reporting to the Information Commissioner's Office (ICO) - see below. To decide, the DPL will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPL will advise the Board of Trustees as appropriate.

Examples of data breaches

The following is a list of possible, but not exhaustive data breaches:

- Loss through fire or flooding

- Loss through accidentally putting down and not knowing where it has gone
- Theft of documents from office, car or home
- Loss of electronic file(s): unable to locate or accidentally deleted
- Loss of data through virus or other malicious malware, or cyber attacks
- Unauthorised access to electronic equipment
- Loss of electronic equipment: laptop, tablet, smartphone, mobile phone, external hard drive, memory stick, DVD, Video

Deletion and destruction of records

All confidential or potentially confidential information must be securely destroyed. Any data, in particular paper documents or notes, disposed of incorrectly may result in disciplinary action.

Paper

If you are disposing of paper this must be shredded using a crosscut shredder. There is such a shredder at both Coventon Road and Wendover Road. Papers containing confidential information must not be put in the general waste or paper recycling bins, nor must they be torn up or put through a shredder that does not crosscut.

If you have a large amount of paper to be shredded, please contact the Finance team who will arrange for this to be confidentially shredded by a third party.

DVD's and Videos

If you have any information on DVD or video that needs to be disposed of this should be passed to Pace IT Services who will arrange for this to be destroyed confidentially.

Electronic information

Data is not deleted from a computer until the recycle bin has been emptied. This has to be done by the user and is not automatic. In addition, information is not deleted from your emails until deleted from your deleted folder. If you have any questions regarding this, please speak to Pace IT Services.

Electronic equipment

All electronic equipment, i.e. hard drives, laptops, memory sticks, external hard drives etc, must be passed to Pace IT services for cleansing and/or destruction.

Use of printers

Great care must be taken when using printers, as information about pupils or children accessing sessions should not be left on the printer for all to see. Wherever possible, use lock print and use your password to release the document. If you share your password with a colleague, please ensure that the individual only sees documents that they are entitled to see. Information such as

IEPs or session reports should not be left lying about, as these could be read by someone who should not have access to the information or be lost because they are not collected in a timely manner.

This loss could be considered a data breach and, if reported, the staff member could be disciplined for not properly controlling and securing confidential information.

Controller Breach Notification to Supervisory Authority

The DPL will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).

The DPL will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPL will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPL will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPL must notify the ICO.

The DPL will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on Pace's SharePoint at https://thepacecentre.sharepoint.com/:f:/s/strategicteam/Ev9yDDhYNBpHqdkSxLe8_LYBBh_kmD_zdNYrnODzlZ6huw?e=K8aDoe.

In the case of a personal data breach, the DPL shall without undue delay and, where feasible and not later than 72 hours after having become aware of it, notify the personal data to the supervisory authority competent in accordance with GDPR Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Notification shall at least:

- Describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
- Communicate the name and contact details of the Data Protection lead where more information can be obtained
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with the rule.

The DPL will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPL will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPL
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPL will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPL will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored on Pace's SharePoint.

The DPL and the Leadership Team will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

Pace will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPL will ask Pace IT services to recall it
- In any cases where the recall is unsuccessful, the DPL will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPL will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- A separate policy has been prepared on the use and security of laptops.

Notification checklist

If a data breach is known or suspected the DPL must be informed. Where the personal data breach is likely to pose a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

DATA BREACH INCIDENT FORM	
Summary of incident	
Date and time of incident	
Number of people whose data is affected (approximate if not known)	
Nature of breach e.g. theft / disclosed in error / technical problems	
Description of how the breach occurred.	
Reporting	
When was the breach reported?	
How did you become aware of the breach?	
Has the Data Protection Lead been advised?	
Personal data	
Full description of personal data involved (without identifiers)	
Number of individuals affected	
Have all the affected individuals been informed?	
If not, state why not	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details	
Data retrieval	
What immediate remedial action was taken?	
Has the data been retrieved or deleted? If yes, state the date and time	
Impact	
Describe the risk of harm to the individual as a result of this incident	
Describe the risk of identity fraud as a result of this incident	

Have you received a formal complaint from any individual affected by this breach? If so, provide details	

DATA BREACH INCIDENT FORM	
Management	
Do you consider the employee(s) involved has breached information governance policies and procedures?	
Please inform of any disciplinary action taken in relation to the employee(s) involved	
Have the employee(s) completed regular data protection training? If so, when? If not, why?	
As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been taken to address this?	
Has there been any media coverage of the incident? If so, please provide details	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure	
Were you aware of weaknesses in the systems, policies or procedures	

breached? Either by audit recommendations or anecdotal evidence?	

This policy will be kept under review and updated as required.

Ian Sansbury, Chief Executive and Data Protection Lead

Last reviewed: December 2022