# PP Data Breach Policy

| | |
|---|---|
| Description | **Data Breach Reporting Policy** |
| Author | **Sarah Bolton** |
| Version | **1.3** |
| Version date | **9th March 2021** |

# Data Breach Policy

## Introduction

**Point Progress**

**1st Floor, Nantwich Court, 5A Hospital Street, Nantwich, Cheshire, CW5 5RH**

This policy sets out the obligations of Point Progress and the processes in place, in the event of a data breach (either internally or externally).

The Company is committed to the letter and spirit of the law, placing high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy and trust of the people with whom it deals.

Our policy is set out as per the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

## Data Breach notifications

All personal data breaches must be reported immediately to the Company's data protection officer (Richard Coope).

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.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you do not need to report the breach, you need to be able to justify this decision, so it must be documented.

A data breach of any kind must be recorded in the Personal Data Security Log. Please use the data reporting guidelines below to inform the Office Manager of the nature of the breach, which can then be recorded.

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

On becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

When reporting a breach, the GDPR says 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 (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely 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.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. You should also remember that the ICO has the power to compel you to inform affected individuals if we consider there is a high risk. In any event, you should document your decision-making process in line with the requirements of the accountability principle.

When notifying individuals you need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer (Richard Coope) or other contact point where more information can be obtained;
- a description of the likely 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 and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection

officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

| Version | Date | Description | Approved By |
|---|---|---|---|
| 1.0 | 07/03/2018 | Initial Policy Drafted | |
| | 07/01/2019 | Policy updated | |
| 1.2 | 19/06/2019 | Policy updated | |
| 1.3 | 09/03/2021 | Policy reviewed & updated | |