Data Breach Management Policy

Introduction

I, Anne Riggs, hold personal and sensitive data on approximately 8 individuals. As a setting, I take every care to ensure the data we hold is managed securely and make every effort to avoid data breaches. In the unlikely event of a data breach, I will take immediate action to minimise any associated risk. In line with best practice and legislative requirements, I will report significant breaches to the Information Commissioners Office (ICO), Ofsted and/or Plymouth City Council, where appropriate.

Purpose

This data breach management policy sets out the course of action I will follow in the event of any data breach or near miss.

Legislation

This policy is written in accordance with the Data Protection Act 2018, incorporating the General Data Protection Regulations (GDPR).

Personal and sensitive data

I use the definitions of personal and sensitive data as defined in the Data Protection Act 2018:

§ personal data means any information relating to a person who can be directly or indirectly identified through the information available. This includes an individual's name, and online identifiers (such as email addresses, IP addresses and cookies).

§ sensitive personal data means any information relating to 'special categories' including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric (computer) data, health data. I understand that such data cannot be processed unless specific conditions exist, for example, I have consent; or there is a legitimate interest (where there genuine reason for me to hold information which may override the right of the individual e.g. to prevent fraud); or a legal purpose for processing such.

Breach definition

For the purposes of this policy, I define a data breach as:

§ any event where a person gains access to information or data that they are not authorised to access. This includes information in any format (for example, paper or electronic), and breaches where an individual's job role does not permit them to access specific information.

§ any event where information (or access to information) is lost and can no longer be used for its intended purpose. This includes information that has been lost, accidentally deleted (where it cannot be recovered), and information which has become corrupt.

§ any situation where information has been changed by unauthorised people or actions, resulting in the information becoming invalid or not fit for purpose (an integrity breach).

§ any other event which breaches the Data Protection Act 2018. This includes re-identifying people (combining anonymous data with other available data to identify an individual).

Data protection breaches can be caused by a number of factors including loss or theft of data and/or equipment on which data is stored; unauthorised access to data; equipment failure; human failure; hacking or unforeseen circumstances such as fire or flood.

Breach classification

I classify data breaches as follows:

§ sensitive electronic/paper data disclosure

§ electronic/paper data disclosure

§ data disclosure near miss

§ other data disclosure - this includes breaches involving conversations and voicemail

§ third party breach

§ lost sensitive electronic/paper file

§ lost non-sensitive electronic/paper file

§ interity threat (threat to the validity/reliability of data e.g. through human error, bugs, viruses etc).

I also record 'near miss' events, for example, where data is sent to an unauthorised person, but is retrieved before it has been accessed. This enables any lessons learnt to be applied, and reduces the number of actual breaches and the impact of such breaches as a whole for our organisation.

Breach management

I will follow the steps below in the event of a data breach. NB. Some steps may take place alongside or at different stages dependent on the individual breach.

Identification:

I will use this policy to ensure all breaches or near misses are identified. Breaches may be identified from self-reporting; reports from parents and carers; and reports from third parties or through other monitoring procedures.

Containment:

I will ensure as a priority that any incident is contained to prevent any further disclosure. This may include taking immediate actions, such as recalling an email or preventing further access to a system.

I will further assess the situation to determine if additional actions are required to minimise the effect of any breach. This may include alerting parents or third parties.

Where we believe an illegal activity has occurred, or is likely to occur, the police will be notified Where security passwords or entry codes have been compromised, such details will be changed immediately and relevant agencies informed.

Impact analysis

I will analyse the breach to determine what the potential impact will be. This will include the personal impact on any individual where appropriate.

Investigation

Once the breach has been contained, I will fully investigate the breach.

The investigation will determine whose data was involved, the potential impact on the data subject and what further steps need to be taken to remedy the situation and prevent recurrence. Although each investigation may differ dependent on the type of breach involved, the following general points will always be considered:

§ the type of data involved

§ the sensitivity of data

§ what protections are/were in place (for example, encryption)

§ what happened to the data

§ whether the data could be put to any illegal or inappropriate use

§ how many people are affected

§ what type of people have been affected (for example, children, practitioners, parents, or suppliers); and whether there are any wider consequences to the breach.

I will keep a clear record of the breach and the actions taken to mitigate it. Any investigation will be completed as a matter of urgency and, wherever possible, within five days of the breach being discovered or reported. Iwill undertake a further review of the causes of the breach on conclusion of the investigation and will consider actions for future improvements at such time.

Notification

I will notify the subject of the breach as soon as possible as part of the initial containment process. The need for further notifications may be identified through the investigation process.

Escalation

I will risk assess each breach on an individual basis. A decision to escalate the breach will be based on the potential impact of the breach on the individuals concerned and the organisation as a whole. In the case of a significant breach, the ICO will be notified. Other agencies, such as Ofsted and Plymouth City Council, will be notified where appropriate. Our insurance company will also be notified where required.

In the case of a cyber-compromise, the National Cyber Security Centre and the police will be notified.

Remediation and implementation

I will ensure any identified remedies, such as changes to procedures, are implemented in a timely manner to prevent recurrence.

Closure

I will only close an incident once we are satisfied that all appropriate management action has been taken. The incident can only be closed on the authority of the setting manager or registered person.

Policy review

This policy may need to be reviewed after a breach or after legislative changes, including new case law or new local or national guidance. As a minimum this policy will be reviewed annually.