Data Breach Response Policy

Approved by Audit Committee 12 May 2020

INTRODUCTION

This policy is designed to ensure The Blessed Christopher Wharton Catholic Academy Trust, its employees, agents and contractors can identify data breaches and meet the requirements of Data Protection Legislation in the handling of a personal data breach (henceforth "personal data breach" or "data breach").

Data Protection Legislation means the Data Protection Act 2018 which incorporates the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the General Data Protection Regulation which is the governing legislation that regulates data protection across the EEA. This includes any replacement legislation coming into effect from time to time.

A personal data breach is defined within the Data Protection Legislation as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental actions by a controller or processor or their employees, agents or contractors;
- human error affected personal data
- sending personal data to an unauthorised recipient;
- network intrusions
- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- alteration of personal data without permission;
- loss of availability of personal data

The notification requirements associated with data breaches rest on the level of risk to the rights and freedoms of data subjects arising from the breach. Unless a personal data breach is unlikely to

This document contains confidential commercial information. Copies should not be taken without prior consent.

result in a risk to the rights and freedoms of the concerned data subjects, it is to be reported to the ICO or relevant supervisory authority. Where such data breaches are likely to result in a high risk to the rights and freedoms of the concerned data subjects, the affected data subjects are to be informed in addition to the supervisory authority.

The Data Protection Legislation further stipulates that where notification of the supervisory authority is required, this should take place within 72 hours of the controller becoming aware of the personal data breach. In the case of breaches which pose a high risk to data subjects, the additional requirement to notify data subjects must be done as soon as possible and without undue delay.

In light of these requirements, this policy focuses on the responsibilities of all employees, agents and contractors associated with the DPO Centre in internally reporting breaches and the external notification requirements.

DEFINITION OF TERMS USED WITHIN THIS POLICY

a. Any reference to “Article” or “Articles” is a reference to an Article or Articles of the “GDPR”.

b. The terms ‘personal data’, ‘data subject’, ‘processing’, ‘pseudonymisation’, ‘controller’, ‘processor’, ‘recipient’, ‘third party’, ‘consent’, ‘personal data breach’, have the meanings set out in Article 4 of the GDPR.

c. “Security incident” means an incident in which the security of personal data may have been compromised but no risk is identified in respect of the rights and freedoms of data subjects. Security incident in the context of this policy may also be used to define an event or action which may compromise the confidentiality, integrity or availability of systems or data, where such event or action does not presently amount to a reportable data breach.

BREACH DETECTION AND REPORTING

A personal data breach or security incident may be detected by any individual who accesses or interacts with systems, records and information belonging to or in the possession of the DPO Centre. As such, all employees, agent, contractors and processors of the DPO Centre are responsible for reporting any suspected or actual security incident or data breach.

All security incidents and data breaches, suspected or actual must be reported to The DPO Centre Ltd, 50 Liverpool Street, London, EC2M7PR. Tel 0203 7971289 and admin@bcwcat.co.uk immediately upon detection. This includes any incidents or data breaches detected outside normal working hours.

When reporting a security incident or personal data breach, suspected or actual, the reporter is obliged to disclose all information within their knowledge using the Breach Report Form annexed to this Policy (Annex 1).

Employees, agents and contractors of the DPO Centre must report all incidents, including those resulting from human error and those with unidentified or unknown affected data subjects as soon as detected.

BREACH INVESTIGATION

The DPO Centre aims to complete a preliminary investigation of all reported incidents without undue delay. The DPO Centre aims to establish its awareness of a personal data breach within the first 24 hours of internal detection. Awareness can be established once it is determined that the reported security incident involves personal data which may be compromised as a result of the

security incident. From this point, there are 72 hours within which to identify whether there is a risk to the concerned data subjects and where there is a risk, notification to the supervisory authority should take place.

During the initial investigation, the DPO Centre aims to establish the following:

- The facts of the security incident
- The data or records concerned
- The value and sensitivity of the data or records concerned
- The type of breach suspected (confidentiality, availability, integrity)
- The number and identity of affected data subjects
- The likely consequences of the breach
- The measures required to contain the impact of the breach

NOTIFICATION TO THE SUPERVISORY AUTHORITY

All personal data breaches which pose a risk to the rights and freedoms of data subjects will be reported to the Information Commission's Office (ICO). The DPO Centre aims to ensure all such notifications are made within 72 hours of becoming aware of the personal data breach.

All notifications to the ICO must be made with the authorisation of an executive employee of the DPO Centre and will be made using the breach notification form provided by the ICO.

COMMUNICATING HIGH RISK DATA BREACHES

Where a high risk to the rights and freedoms of data subjects is established, the DPO Centre will inform data subjects of the personal data breach as soon as possible and without undue delay. Communication to data subjects should include:

- The nature of the breach
- The name and contact details of the DPO or other contact person
- The likely consequence of the breach
- The measures taken or proposed to be taken by the controller to address the breach
- any recommended steps to be taken by the data subjects themselves e.g. changing passwords

The DPO Centre aims to notify data subjects of relevant personal data breaches directly unless it is impossible to do so, or it would involve a disproportionate effort, in which case the breach may be communicated by way of a public statement. All such communications must be authorised by an executive employee.

ACCOUNTABILITY

All security incidents reported will be documented regardless of whether the breach was notifiable to the ICO. The DPO Centre will maintain a breach register containing all reported incidents.

This document contains confidential commercial information. Copies should not be taken without prior consent.

Annex 1

Please complete this form if you have detected or been advised of a data breach. It is imperative that you complete this form immediately upon detection and where possible, please advise your line manager of the suspected breach immediately.

Once completed, please email this form to **advice@dpocentre.com** and **admin@bcwcat.co.uk**

Incident / breach details	
Name of person reporting incident:	
Contact details of person reporting incident:	
Date(s) incident took place:	
Date you detected the incident:	
Place of incident:	
Brief description of how you became aware of the incident:	
Brief description of the incident including details of the data, records or systems believed to be affected:	
Approximate number of affected data subjects, if known:	

Approximate number of affected records, if known:	
Any actions taken in response to the incident:	