Author: CGK
Committee: Audit
Approved by Governors: Feb 2020
Committee Review Date: Feb 2023
Statutory Policy
Review Frequency – every three years

Birchwood High School
Data Breach and Information Security Incident Management Policy and Procedure

Executive Summary

Birchwood High School makes all efforts to ensure the security of its information systems and the Personal Data for which it is responsible. This policy will ensure that where incidents occur, they are managed in a way that supports compliance with the School's legal obligations and individuals' rights. All users of Birchwood High School's Information and information systems are required to familiarise themselves with and comply with this policy.

Definitions of terms are at part 13.0 of the policy.

- An Information Security Breach is an incident which has caused or has the capacity to cause unauthorised disclosure of and / or damage to Birchwood High School's Information, information systems or reputation. Examples are at part 7.1 of the policy, and include:
- Accidental loss or theft of data or equipment
- Unauthorised or accidental use, access to or modification of data or information systems
- Unauthorised or accidental disclosure of data
- Compromised user accounts or attempts by criminals to gain access to or disrupt data or systems
- Equipment failure
- Some of these incidents may involve Personal Data, in which case these are defined as Personal Data
    - Breaches. Examples are at part 7.2 of the policy, and include:
- Unauthorised or accidental disclosure of personal data
- Accidental or unauthorised loss or theft of personal data or equipment
- Damage, destruction, alteration or loss of personal data
- Members of staff discovering incidents must report the incident immediately to the IT Service Desk at itsupport@birchwoodhigh.org.uk, extension 3232, also to their Line Manager or SLT.
- Reports of Personal Data breaches must also be reported to dpo@birchwoodhigh.org.uk
- Details should be provided using the Incident Reporting Form
- More information is at part 8.0 of the policy.
- An incident management team made up of relevant people will investigate and assess the risks involved in the incident, and will attempt to contain the incident and / or recover systems or data losses.
- External bodies (e.g. the Information Commissioner) will be notified if necessary. Data Subjects will be notified if a high risk has been identified.

Data Breach and Information Security Incident Policy and Procedure

Introduction

1.1 Birchwood High School's utilises various information systems and holds a large amount of data / information which may include personal or confidential information (about people), and also non-personal information which could be sensitive or commercial, for instance financial data.

1.2 Care should be taken to protect this Information and information systems from incidents (either accidental or deliberate) that could compromise their security.

1.3 In the event of a data breach or an information security incident, it is vital that appropriate actions are taken to minimise associated risks.

Purpose

The purpose of this policy is to set out the procedure that should be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across t Birchwood High School.

Scope

This policy applies to all Birchwood High School's staff, students, contractors and third party agents handling Birchwood High School's Information and information systems.

Relationship with other policies

This Policy is related to the following policies:
a) General Data Protection Policy
b) Acceptable use of ICT Policy

Responsibilities

5.1 All users of Birchwood High School's Information and information systems are required to familiarise themselves with and comply with this policy.
5.2 All individuals who access, use or manage Birchwood High School's Information and information systems are responsible for reporting data breach and information security incidents -see point 8.0 below.

Compliance

6.1 Birchwood High School has an obligation to comply with relevant statutory, legal and contractual requirements. The Data Breach and Information Security Incident Policy and Procedure is part of the Information Security suite of policies, designed to ensure data breach and information security incidents are reported promptly and managed properly to mitigate any risks to the confidentiality, integrity and availability of Birchwood High School's Information and information systems.
6.2 Failure to adhere to this policy will be addressed by necessary disciplinary actions in accordance with the Staff Disciplinary Procedures, Student Disciplinary Regulations and Procedures and relevant contractor and third party contractual clauses relating to non-conformance with the Data Security and Policy and related policies.

Definition of an incident

7.1 An incident in the context of this policy is an event which has caused or has the potential to cause unauthorised disclosure of and / or damage to Birchwood High School's Information, information systems or reputation.

- Examples of an Information Security Breach are:
- Accidental loss or theft of sensitive or personal data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised or accidental use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- Unauthorised or accidental disclosure of sensitive or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal data posted onto the website without consent

- Damage or destruction or loss of personal data, or accidental or unlawful alteration of personal data (e.g. due to failure of equipment, or changes or deletions made by staff of documents on shared drives or Birchwood High School's systems)
- Compromised user account (e.g. accidental disclosure of user login details through phishing)
- Failed or successful attempts to gain unauthorised access to Birchwood High School's Information or information systems
- Equipment failure resulting in the non-availability of data
- Malware infection
- Disruption to or denial of IT services

7.2 Some of these examples may result in a Personal Data breach. This is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. While all Personal Data breaches are information security incidents, not all information security incidents are necessarily Personal Data breaches. A Personal Data breach occurs where information relating to identifiable living individuals is involved.

Reporting an incident and record-keeping

8.1 It is the responsibility of the discovering member of staff to report information security incidents immediately to the IT Service Desk at itsupport@birchwoodhigh.org.uk, and extension 3232, as the primary point of contact, so that Birchwood High School is aware that an incident has taken place. Incidents must also be reported to your Line Manager or SLT.

8.2 Reports of Personal Data breaches should be sent without delay to the Birchwood High School's Data Protection officer at dpo@birchwoodhigh.org.uk From 25 May 2018, legislation will require any report to be made to the Information Commissioner's Office (ICO) within 72 hours, and the school's Data Protection Officer will do this if it is necessary. The DPO will also determine whether individual data subjects should be informed about the breach.

8.3 Reports should be an accurate description of the incident, including who is reporting the incident, what type of information the incident relates to, and, if Personal Data is involved, how many people it may affect and the category of people (e.g. Staff, Student, etc.). Details should be provided using the Incident Reporting Form.

8.4 If a computer system breach has occurred, the Network Manager and the DPO will be informed by the IT Service Desk.

8.5 The IT Service Desk will maintain a log of all information security incidents, which will include all stages of the investigation and outcome. The DPO will maintain a log of Personal Data breaches or incidents, which will include all stages of the investigation and outcome.

Investigation and Risk Assessment

9.1 The DPO or nominated alternative will instigate an appropriate incident management team made up of people relevant to the type of incident, or inform the most appropriate individual to investigate the incident. If the incident relates to Personal Data. It will aim to be started within 24 hours of the incident being discovered, where possible.

9.2 The investigation will establish the nature of the incident, the type of data involved, and will consider the extent of a system compromise or the sensitivity of the data. A risk assessment will be performed as to what might be the consequences of the incident, for instance whether data access or IT services could become disrupted or unavailable.

9.3 Where Personal Data breaches are concerned, the risk assessment will consider whether there is a risk involved to individuals. This risk assessment will consider the nature, sensitivity and volume of personal data involved, and the number of data subjects; the ease of identification of individuals from the data; the category of data subject, for instance whether they are a child or a vulnerable person; what might be the consequences of the incident and the severity of the impact this would have and the likelihood of this occurring.
These factors will help to determine whether there is a risk, or a high risk. The risk assessment will determine whether the incident should be reported to the ICO and whether data subjects should be informed.

Containment and Recovery

10.1 The incident management team will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.
10.2 Appropriate steps will be taken to recover system or data losses and resume normal business operation. This

might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

External Notification

11.1 The Principal and Chair of Governors will be notified by the DPO, following a critical data breach involving large amounts of data, or a significant number of people whose Personal Data have been breached.

11.2 The DPO, Principal and Chair of Governors will decide to inform any external organisation, such as the police or other appropriate regulatory body.

11.3 If a breach involving Personal Data has occurred, the Data Protection Officer will inform the Information Commissioner's Office (ICO) if necessary, based on the risk assessment which has been undertaken. If there is considered to be a risk to people's rights and freedoms (under the General Data Protection Regulation) then the ICO will be informed without undue delay and where feasible not later than 72 hours after the University has become aware of the breach.

11.4 Birchwood High School will where possible notify individuals whose Personal Data has been subject to a breach, where a high risk has been identified to those individuals, without undue delay.
High risk situations are likely to include the potential of people suffering significant detrimental effect e.g. discrimination, damage to reputation, financial loss, identity theft, fraud, or any other significant economic or social disadvantage. This will help them to take steps to protect themselves. The notice will include a description of the breach and the steps taken to mitigate the risks.

Review

12.1 Once the incident is contained, a review of the event will be undertaken by the relevant team or individual and reported to DPO, Principal and Chair of Governors.
The report will detail the cause of the incident and contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvement.

12.2 Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

Definitions

- Authorised Users (in the context of this policy and related documents)
  All users who access, handle, process, store, share or manage Birchwood High School's Information. These are Birchwood High School's staff, students, contractors and third party agents.
- Availability
  Information and information systems are accessible only to authorised users when required.
- Confidentiality
  Access to and sharing of sensitive or personal information is restricted only to authorised users.
- Information
  Information is data and recorded knowledge, enabling Birchwood High School to carry out its business. It can be in any format or medium, and can include the content of information systems.
- Information Systems
  Information processing computers or data communication systems.
- Integrity
  The preservation of the complete, accurate and validated state of Information.
- Personal Data
  Personal data relates to living individuals (Data Subjects) who can be identified from it, either by itself or in tandem with other information that might be in Birchwood High School's possession. It includes expressions of opinion, and intentions towards the individual.
- Risk Assessment
  A process for identifying and evaluating risks, either to people's rights and freedoms, or to adverse events within computer systems.
- Sensitive Data
  Personal information concerning: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health, sex life or sexual orientation; or commercial or financial information which would not normally be in the public domain.
- Unauthorised
  Without a legitimate right.

Related Policies, Processes and Standards
Links to the Data Security Policy, Acceptable Use of ICT and related policy documents
Links to the Data Protection Policy and related policy documents
Data Protection Act 1998, to be superseded 25/05/18 by:
The General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679
Privacy and Electronic Communications (EC Directive) Regulations 2003
Report of an Information Security Incident or Data Breach

Members of staff discovering incidents must report an information security incident or Personal Data breach immediately to the IT Service Desk at itsupport@birchwoodhigh.org.uk , extension 3232, also to their Line Manager or SLT. Reports of Personal Data breaches must also be reported to dpo@birchwoodhigh.org.uk Please use this form to provide details of this incident.

Data Breach and Information Security Incident Reporting Form

Person reporting the incident				
Department and contact details				
Date of incident				
Description of incident:				
Is Personal Data involved?	Yes		No	
Categories of personal data (e.g. name, address, ID, etc.)				
Categories of data subject (e.g. student, staff, student applicant)				
Number of data subjects involved (if known)				
Any initial action taken in response to incident				