CHRIST CHURCH DATA BREACH REPORTING POLICY

Introduction

This policy relates to all personal and sensitive data held by the school regardless of format; electronic or paper based.

The school holds, processes, and shares a large amount of personal data, which needs to be protected at all times.

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

All staff should be aware that any breach of the Data Protection Act 2018 or the General Data Protection Regulation (GDPR) might result in the school's Disciplinary Procedures being instigated.

The school is obliged to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definition / Types of Breach

For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

"Personal data breach" under the GDPR covers more than just the unauthorised disclosure of personal information. The phrase is defined 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 by the company"

An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the school's information assets and/or reputation.

Information Security Incidents

An information security incident is a violation or breach of the schools information security policy and associated acceptable use policies or a breach of the IT code of conduct.

A security incident is an event which causes or has the potential to cause:

- Degraded system integrity
- Loss of system or information availability
- Disclosure of confidential information, whether electronic or paper, or any other form including conversation
- Corruption of information
- Disruption of activity
- Financial loss
- Legal action
- Unauthorised access to applications
- Unauthorised access to premises

An incident includes but is not restricted to, the following:

- Attempts (either failed or successful) to gain unauthorised access to a system or its data
- Unwanted disruption or denial of service
- The unauthorised use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Loss of removable media (USB Stick, Disc etc) and portable equipment (Laptops/Tablet PCs)
- Tampering/attempting to tamper with CCTV cameras or the leaking of unauthorised film footage taken from CCTV equipment
- Damage to or theft /loss of ICT equipment or confidential / sensitive papers (either manual or electronic)
- Unauthorised access to confidential / sensitive information in any form including receiving information meant for someone else
- Unauthorised disclosure of confidential / sensitive information in any form to a third party
- Transfer of information to the wrong person (by fax, email, post or phone)
- The finding of confidential information/records in a public area
- The unauthorised usage of another user's security credentials
- Sharing computer ID's and passwords
- Accessing another individual's personal details without permission.
- Leaving confidential / sensitive information on public display
- Virus outbreak.

Reporting an incident

Any individual who accesses, uses or manages the schools information is responsible for reporting the data breach and information security incidents immediately to the school's Headteacher (or deputy) and the Data Protection Officer.

[Schools may modify this process somewhat to suit their own internal workings. The key parts are that a staff member reports to their own leadership ASAP and they have the option to go directly to the Data Protection Officer if leadership are not available or do not adequately respond. Some schools may want to maintain the chain of command so that leadership contacts the DPO. This is acceptable providing that a staff member can bypass this if required.]

The School's Data Protection Officer is Andrew Maughan, Borough Solicitor for the London Borough of Camden. Reports should be made via email schoolsdpo@camden.gov.uk or telephone 0207 974 4365.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon staff become aware of it.

The report should include full and accurate details of the incident;

- when the breach occurred (dates and time)
- the type of data involved
- how many individuals have been affected and the potential effects on those data subject(s)
- who is reporting it
- the protections in place (e.g. encryptions)
- what's happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- whether there are wider consequences to the breach

If the above points cannot be answered, the report should still be made immediately and not delayed in order to establish these details. The School's management and/or the Data Protection Officer will work to identify and remedy any gaps and reporting should not be delayed in order to fill in missing information.

An Incident Report Form should be completed as part of the reporting process (see Appendix 1)

Initial Assessment

An initial assessment will be made by the DPO in liaison with relevant school staff to establish the severity of the breach and to determine roles and responsibilities in responding to the breach.

The DPO will determine a suitable course of action and if deemed necessary, prepare a report for the Information Commissioners' Office (ICO) to be submitted within 72 hours of the breach being detected.

The 72 hour period does not take into account non-working days, weekends, and public holidays.

The ICO will then assess the breach and inform the DPO what further action is required.

Containment and Recovery

The school, advised by the DPO, will firstly determine if the breach is still occurring. If so, appropriate steps will be taken immediately to investigate the breach and assess the risks associated with it.

The staff designated by the DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempting to recover lost equipment.
- The use of back-ups to restore lost/damaged/stolen data.
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation and Risk Assessment

The investigation will need to take into account the following:

Notification

The school, advised by the Data Protection Officer, must decide whether to notify any individuals affected by the Data Breach. It will not always be necessary, or beneficial to do so, but in any cases where there will be a significant risk to the rights or freedoms of the data subject then the subject will normally be notified.

Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the school for further information or to ask questions on what has occurred.

The school, with advice from the DPO, must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The DPO will advise whether the School should make a press release and to be ready to handle any incoming press enquiries.

Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

The school will notify the DPO of all actions taken in response to the breach and the DPO will keep appropriate records.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

The DPO will be responsible for deciding how to report the incident to the School's governing body

Implementation

The Head Teacher should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager or the Head Teacher.

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, notify the Data Protection Officer immediately.

Complete Section 1 of this form and email it to schoolsdpo@camden.gov.uk

Section 1: **Notification of Data Security Breach**	**To be completed by person reporting the incident**
Date(s) of incident	
When was it discovered:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Description of incident or details of the information lost:	
Number of data subjects affected, (if known):	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	