INFORMATION SECURITY

IMPACT ASSESSMENT

Ref:

Completed by - Name	
Job Title	
Date incident happened	
Date incident reported	
Date investigation started	
Date investigation completed	
Brief description of the incident	

Purpose of this assessment

The purpose of this assessment is to:

1. Provide a consistent approach to categorising information security incidents.
2. Determine whether the Information Commissioners Office should be notified about the incident.
3. Provide an overview of the incident for the Head Teacher / Chair of Governors along with recommendations on what action should be taken to address matters and to prevent a reoccurrence.

Although there is no legal requirement on the School to report Information Security incidents which result in the loss, release or corruption of personal information, the Information Commissioner believes serious breaches should be brought to the attention of his office (ICO). The nature of the incident or loss can then be considered by the ICO, together with whether the School is properly meeting its responsibilities under the Data Protection Act.

Serious breaches are not defined. Therefore, using the Information Commissioners own guidance entitled *"Notification of data security breaches to the Information Commissioners Office (ICO) – Ver 1 23 July 2012*" and the Department of Health guidance entitled *"Checklist for Reporting, managing and Investigating Information Governance Serious Untoward Incidents Gateway Ref: 13177 January 2010"*, Solihull Council officers have developed this guidance for internal use in determining the Impact of a particular breach.

This assessment will consider the:

- Sensitivity of the information
- Volume of information
- Potential Detriment to Individuals

Assessing the Impact of the Incident

Overview

Risk assessment models commonly categorise incidents according to the likely consequences, with the most serious being categorised as 5. Using the Department of Health and Information Commissioners guidance the following matrix has been developed to help assess the impact of the incident.

	1	2	3	4	5
Sensitivity	Minor breach of confidentiality but contained to single recipient. No sensitive personal data Breach contained and data retrieved within 2 hours.	As (1) but strong possibility that recipient has disclosed to others.	Unauthorised disclosure of limited personal data. Some sensitive personal data involved	As (3) but strong possibility that recipient has disclosed to others.	Unauthorised disclosure of particularly sensitive data e.g. health records or substantial personal data.
Volume	Up to 5 people affected	Between 6 – 20 people affected or A single individual with a high volume of personal data	Between 21 and 100 people affected or Less than 20 people with a high volume of sensitive personal data	Between 101-1000 people affected or Between 21 and 100 people with a high volume of sensitive personal data	Over 1000 people affected or Between 101-1000 people with a high volume of sensitive personal data
Likelihood of Detriment	No obvious detrimental effect on any individual.	Minor inconvenience for the individual. Potential for individual complaint.	Possibility for limited short term distress. Short term local media attention. Possibility of limited financial damage. Limited short term embarrassment.	Limited longer term distress. Sustained local media coverage. Possibility for ID theft or fraud.	A real risk of serious harm or substantial longer term distress. National media coverage. Strong possibility for ID theft, fraud and/or substantial financial damage. Highly embarrassing.

When to Report

As a rule, any incident that scores 10 or above will need to be reported to the Information Commissioner Office. The loss of encrypted media / equipment will not need to be reported.

Assessing the Impact of the Incident

1

Provide a summary of the incident, and findings for the 4 stages of the investigation (1. Containment & Recovery, 2. Risk Assessment, 3. Notification and 4. Evaluation and Response).

OVERVIEW

Briefly the describe the incident

CONTAINMENT

Summarise the actions taken to recover from the mistake, e.g. collected information, or asked recipient to delete it.

RISK

Describe the risks that were posed by the error; for example, if the information contained financial data such as bank account numbers then there may be a risk of fraud, or if the information contained sensitive health and personal data there might be a safeguarding issue

NOTIFICATION

If there is anyone that needs to be notified, list them below and state why; notifying a person whose information got misdirected, for example, would help them take precautions against ID theft, fraud etc. Also consider if notification would serve only to worry them without any benefit.

EVALUATION AND RESPONSE

Summarise the lessons learnt as well as how this will be prevented from happening again

Assessing the Impact of the Incident

2

Head Teacher / Chair of Governors Decision, Recommendations and Sign off

The Head Teacher / Chair of Governors have read the Report into the matter and discussed the matters with relevant members of staff to reach the below conclusions:

1: The incident is scored as _____ on the impact matrix and is / is not [delete as applicable] reportable to the Information Commissioner.

2: [Add additional points as required]

Head Teacher / Chair of Governors [delete as applicable]