Discovery Schools
Academy Trust

# Data Security Incident Management Policy and Process

# April 2018

**Document Version: V2**
**Review Date: May 2019**

**Owner: Director of Operation**

**Document History**

| Date | Author | Version Number | Summary of changes |
|---|---|---|---|
| 27th March 2018 | Director of Operations | V1 | New draft policy – v1 |
| 16th April 2018 | Director of Operations | V2 | Revised in consultation with Director of IT |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Contents

## 1. Introduction

**Discovery Schools Academies Trust (DSAT),** further referred to as **DSAT** or **the organisation** has a responsibility to ensure that data is protected. A breach in information security could cause serious harm to employees and the wider organisation stakeholder.

Inappropriate handling of personal data, information processing systems and equipment could lead to information breaches which have financial and legal implications and could cause reputational damage to the organisation. The risk associated with an information breach is high for DSAT due to the personal and/or sensitive nature of much of the data processed by the authority.

An information security incident is any occurrence that could compromise the confidentiality, integrity (i.e. accuracy and completeness), or availability of information. This includes information stored and processed electronically, and information stored or transmitted in other forms, such as on paper. Any such incident must be reported for investigation and appropriate security controls should be implemented to mitigate or minimise risks and avoid a recurrence.

Information security incidents include, but are not limited to the following:-

- The loss or unauthorised disclosure of personal or sensitive information.
- Transfer of sensitive information to those who have no need to see it.
- Attempts (failed or successful) to gain unauthorised access to information or a computer system.
- Unauthorised changes to information or system hardware/software.
- Loss or theft of ICT equipment including peripheral storage items e.g. USB memory devices.
- Unauthorised use of a system (electronic or manual) for processing/ storage of data by any person.

The necessity to report and manage information security incidents at an organisational level is underpinned by the need to prove our assurance arrangements for data to the public and for personal data to the Information Commissioner who is empowered where there is a Data Protection breach to levy monetary penalty notices of up to £500,000 and require remedial action.

This policy also covers the management of information security incidents relating to the inappropriate use of CCTV data and equipment which could be breaches of the ICO CCTV Code of Practice or the Protection of Freedoms Act. Owners and operators of CCTV are responsible and accountable for correctly operating CCTV systems and controlling the CCTV data within their facilities. Instances where principles as defined within the CCTV Code of Practice are not being adhered to should be reported as part of this process.

## 2. Purpose

The purpose of this policy is to provide guidance on how information security incidents should be handled and reported and to identify the roles and responsibilities of key personnel in the investigation of such incidents. The aim of this document is to ensure that relevant and prompt action is taken on actual or suspected information security related incidents to minimise their impact and the risk of recurrence.

## 3. Scope

The policy applies to:

- DSAT employees, contractors, partners and suppliers.
- Information assets, whatever format, device or medium they are held in.
- All DSAT owned information, in whatever format, wherever it is held (e.g. by a third party) for which DSAT is the data controller.

## 4. Roles and responsibilities

**Appendix 1** highlights the key roles and responsibilities for Information Security Incident Management within the organisation.

## 5. Information Security Incident Management Process

**Appendix 4** illustrates the Information Security Incident Management Process detailed below.

### 5.1 Incident Reporting

Reports of a potential security incident may come from an internal or external source.

When an incident or suspected incident is identified, the Director of Operations (DoO) must be informed. The person reporting the incident (ideally the Local Data Protection Representative LDPR) should complete an 'Information Security Incident Form' (see **Appendix 3**) within 24 hours of the incident and submit the completed form lbarber@discoveryschoolstrust.org.uk so that the incident can be further investigated.

Upon receipt of the 'Information Security Incident Form' the DoO will make a decision on whether this is an information security related incident and may contact the LDPR for further information where required. The LDPR must give as much detail as possible (e.g. the date of the incident, who was involved, the information concerned, etc.).

Where information security incidents relate to IT, e.g. an actual or suspected technical attack on systems or the loss of IT equipment, they should be logged with the Director of IT via the IT Helpdesk who will then notify the DoO.

### 5.2 Investigation

If it is identified that the information security incident warrants further investigation, the DoO will nominate an individual from the DSAT organisation concerned to lead and undertake the investigation, engaging key stakeholders where required. If the nominated officer is uncertain on the key stakeholders that should be engaged, advice should be sought from the DoO.

The nominated officer assigned the task of undertaking the investigation, should, with advice (where required) from the DoO and other stakeholders:

- Ensure that personnel with the appropriate knowledge and technical expertise are involved where there is a requirement for retrieval of information or recovery of systems/ equipment.
- Determine whether there are any third parties involved or affected by the incident e.g. other authorities, suppliers, etc.
- Prepare an investigation report and forward this to the CEO and the Executive Team for communicating to the Board of Directors.
- Liaise with HR to consider whether an investigation under the disciplinary procedure is appropriate and required.

### 5.3 Preventing recurrence

Once the incident has been investigated, any lessons that can be learned from the incident should be highlighted. This is so that any gaps in security can be identified and controls put in place to minimise the risk of recurrence of the incident. This should be done by the Executive Team and other key stakeholders. Recommendations for improving controls will be made and the implementation of these actions will be tracked by the DoO.

### 5.4 Reporting to senior management and regulatory bodies (eg. ICO)

Where an incident is deemed to be serious, this would need to be reported to the CEO and the Board of Directors.  A decision will then be made as to whether the incident needs to be reported to relevant regulatory bodies, notably the Information Commissioners Office (ICO) (for incidents involving personal data). This reporting will be handled by the DoO and LDPR should not contact the ICO without contacting DoO first..

### 5.5 Incident log

All information security incidents reported will be recorded on the Information Security Incidents log held by school and partner offices. A log is updated and maintained by all local schools and DSAT offices and is used for trend analysis and wider summarised reporting conducted by the data protection officer DPO. The log categorises incidents to enable meaningful reporting.

All reports are incidents, but only subsets of these are 'data breaches' or 'breaches' (where data has actually been compromised). In turn, only subsets of the breaches are breaches of the GDPR (those involving person identifiable data).

## 6. Policy review

This policy has been agreed and distributed for use across the organisation by the Finance, Audit and Risk Committee. It will be reviewed annually by the DPO , who will forward any recommendations for change to the Board of Directors for consideration and distribution.

**Appendix 1: Roles and Responsibilities**

| Role | Responsibilities |
|---|---|
| All employees | • Comply with DSAT policy and legal requirements relating to information security and GDPR regulations.<br>• Report any incidents/ potential incidents likely to cause a breach of the organisations's policies and/or legislation.<br>• Raise any unusual security-related occurrences with their relevant line manager.<br>• Contribute to investigations as and when required.<br>• Ensure evidence of an information breach is not damaged. |
| SLT in school and Exec team for ATSA/SCITT/EPIC/DSAT | • Ensure all staff are aware of the Information Security Incident Management Process.<br>• In the event of an incident, formally report (i.e. complete the incident form) and submit this to the Director of Operations – lbarber@discoveryschoolstrust.org.uk<br>• Contribute to investigations as and when required.<br>• Implement controls as suggested in order to prevent/minimise the risk of incidents reoccurring.<br>• Review and amend policies and procedures to reduce the risk of incidents occurring<br>• Seek security advice from DoO and the Director of IT where required<br>• Keep all other relevant stakeholders informed throughout the incident process<br>• Liaise with central HR to determine if an investigation under the disciplinary procedure is required. |
| Nominated Incident co-ordinator | • Undertake the investigation<br>• Complete an incident report for submission to the DoO<br>• Involve key stakeholders in the investigation as and when required and keep them informed<br>• Seek advice from specialist areas where required |
| ICT Services | • Pick up any initial calls relating to incidents and notify the DoO<br>• Monitor technical facilities to detect potential security incidents.<br>• Implement the Incident Process or Major Incident Process if warranted by the incident.<br>• Conduct technical investigations and recovery of information systems following an information security incident.<br>• Regularly review procedures and technical configurations to reduce the risk of incidents occurring.<br>• Implement controls as recommended.<br>• Communicate any system down time/ issues to users. |
| DPO | • Provide support to relevant stakeholders as appropriate during investigations.<br>• Support Director of Operations when reporting to ICO.<br>• Share best practice.<br>• Undertake reviews to ensure controls are working as intended. |
| Central HR / Legal | • Support managers on any HR/legal issues when undertaking investigations.<br>• Liaise with key stakeholders as appropriate during investigations.<br>• Work with DoO to help improve controls, policies and procedures. |
| Director of Operations | • Co-ordinate/undertake investigation when required. |

| | |
|---|---|
| | • Provide advice to the nominated officer undertaking the investigation.<br>• Keep the incident log up to date and track the tasks delegated to officers.<br>• Keep all other relevant stakeholders informed throughout the incident process.<br>• Where applicable, report incidents to the Information Commissioner's Office once agreed with the CEO<br>• Ensure follow up actions from incidents are being completed<br>• Regularly review and update the Information Security Incident Management Policy and Process<br>• Advise on mitigating controls that can be implemented to prevent reoccurrence of incidents<br>• Provide advice on information Security Incident Management and ensure relevant documentation is completed in the event of an incident |
| CEO | • Be made aware of incidents, outcomes and recommendations.<br>• Obtain assurances that follow up actions are carried out.<br>• Acts as appropriate on issues encountered within investigations or in implementing remedial recommendations.<br>• Authorise the reporting to the Information Commissioner where required |
| Board of Directors | • Receives a summarised list of incidents, outcomes and recommendations for scrutiny<br>• Ratify the Information Security Incident Management Policy and Process<br>• Be made aware of serious incidents, their outcomes, recommendations and completion of actions where there is a possible requirement to report to the ICO |

**Appendix 2: Severity Table**

NB: This table only gives broad guidelines on the severity of incidents. Each case may differ depending on other variables e.g. the number of people affected, the type of information concerned etc. The severity of each incident should therefore be considered on an individual basis.

| **Incident Type** | **Breach of** (Confidentiality, Integrity, Availability & Accountability) | **Severity** |
|---|---|---|
| Unauthorised access to Network/ Systems/ Applications/ Email | Integrity/ Confidentiality/ Availability & Accountability | Moderate to Major depending on the level of information accessed |
| **Sending information** | | |
| Information sent to the wrong recipient (internally), disclosing information that is neither confidential not personal | Integrity | Minor |
| Information sent to various recipients (including external recipients) disclosing non confidential or non-personal information | Integrity | Moderate |
| Information sent to an unauthorised recipient(s) containing confidential and sensitive personal information (whether Internal or External) | Integrity/Confidentiality | Major |
| **Loss of equipment** | | |
| Loss or theft of equipment containing no confidential and/or personal information | Availability | Minor/ Moderate |
| Loss and theft of equipment containing confidential and/or personal information but with encryption software installed on the equipment | Availability/ Confidentiality | Moderate |
| Loss and theft of equipment containing confidential and/or sensitive personal information where equipment has no encryption software installed | Availability/ Confidentiality | Major |
| Inappropriate material found on PC | Accountability | Minor to Major depending on the type of material found on the PC |
| Illegal material found on PC | Accountability | Major |
| Inappropriate/unauthorised use of the network/software leading to a disruption of services | Availability | Major |
| Inappropriate use of the internet or email as defined within the AUP Policy | Accountability/ Availability | Minor to Major depending on the circumstances |
| Passwords written down leading to unauthorised access | Integrity/ Confidentiality/ Availability & Accountability | Moderate/ Major depending on the type of information and system and impact of the incident |
| Offensive emails being sent | Accountability | Moderate to Major depending on content of the email |
| Spam or 'phishing' emails | Availability | Minor to Moderate depending on the impact and number of users affected. |
| Information sent externally or internally by fax, post or hand (containing no confidential or personal information) is lost | Availability | Moderate |

| | | |
|---|---|---|
| Information sent externally or internally by fax, post or hand (containing confidential or sensitive personal information) is lost | Integrity/ Confidentiality/ Availability & Accountability | Major |
| Unintentional corruption of data | Availability | Moderate/Major depending on the amount of data and type of data corrupted |
| Intentional corruption of data | Availability and Accountability | Major |
| Password sharing | Accountability/ Integrity/ Confidentiality | Moderate to Major depending the type of data in question |
| Downloading or copying of unlicensed software | Accountability | Major |
| Information/ data deleted or amended from a database in error | Accountability/ Integrity & Availability | Moderate |
| Information/ data deleted or amended from a database maliciously | Accountability/ Integrity & Availability | Major |
| Confidential information disposed of inappropriately | Accountability | Major |
| Website Hacked | Availability/ Integrity | Moderate to Major depending on the criticality of the system |
| Misuse of Telephony Service | Accountability | Minor to Major on the level of misuse |

## Appendix 3 - Information Security Incident Reporting Form

**Information Security Incident Reporting Form**

**Email completed forms as soon as possible to lbarber@discoveryschoolstrust.org.uk**

**Provide as much information as you can, but do not delay sending in the form. For urgent incidents (e.g. virus infection), phone the IT Helpdesk straightaway:**

| | |
|---|---|
| **GENERAL DETAILS** | |
| **Incident number:** | *To be added by DoO for easy reference* |
| **School/DSAT location:** | |
| **LDPR:** | |
| **Investigated by:** | |
| **Contact number:** | |
| **Date form completed:** | |
| **Date of incident:** | |
| **ABOUT THE INCIDENT** | |
| **Incident description. What has happened?** | |
| **How was the incident identified?** | |
| **What information does it relate to?** e.g. a file containing details of 100 service users name, address, direct debit details. | |
| **What medium was the information held on?**<br>• Paper<br>• PEN/Memory stick<br>• laptop, etc | |
| **If electronic, was the data encrypted?** | |
| **Dealing with the current incident:**<br>**Please list initial actions: -**<br>• Who has been informed?<br>• What has been done? | |
| **Are further actions planned?** If so, what? | |
| **Have the staff involved in the security incident done any Data Protection Training?** | Yes / No |
| **If so, what and when? (Please list)** | |
| **Preventing a recurrence:**<br>**Has any action been taken to prevent recurrence?** | |
| **Are further actions planned?** If so, what? | |

| | | |
|---|---|---|
| **IMPACT ASSESSMENT QUESTIONS** | | |
| 1. | **Was any data lost or compromised in the incident?**<br>e.g. loss of an encrypted laptop will not actually have compromised any information, unless e.g. the user was logged in when they lost it. | Yes/No |
| **2.** | **Was personal data lost or compromised?** | Yes/No |

| | | |
|---|---|---|
| | This is data about living individuals such employees, pupils and parents. This could be a breach of the Data Protection Act 1998. | |
| **3.** | **If yes, was <u>sensitive</u> personal data compromised?**<br>This is data relating to health, ethnicity, sexual life, trade union membership, political or religious beliefs, potential or actual criminal offences.<br>This could be a serious breach of the Data Protection Act 1998. | Yes/No |
| **4.** | **Was safeguarding, Child Protection data involved?** | Yes/No |
| **5.** | **What is the number of people whose data was affected by the incident?** | |
| **6.** | **Is the data breach <u>unlikely</u> to result in a <u>risk</u> to the individual/individuals? Physically, materially, or morally?**<br>Example - physical harm, fraud, reputation, financial loss, | Yes/No |
| **7.** | **Did people affected by the incident give the information to the organisation in confidence?** (i.e. with an expectation that it would be kept confidential) | Yes/ No |
| **8.** | **Is there a risk that the incident could lead to damage to individuals eg. via identity theft/ fraud?** E.g. loss of bank details, NI numbers etc. | Yes/No |
| **9.** | **Could the incident damage an individual's reputation, or cause hurt, distress or humiliation e.g. loss of medical records, disciplinary records etc.?** | Yes/No |
| **10.** | **Can the incident have a serious impact on DSAT's reputation?** | Yes/No |
| **11.** | **Has any similar incident happened before at this location?** | Yes/No |
| **13.** | **If this incident involves the loss or theft of IT Equipment please confirm you have logged a call on the ICT Help & Support helpdesk?** | Yes/No |

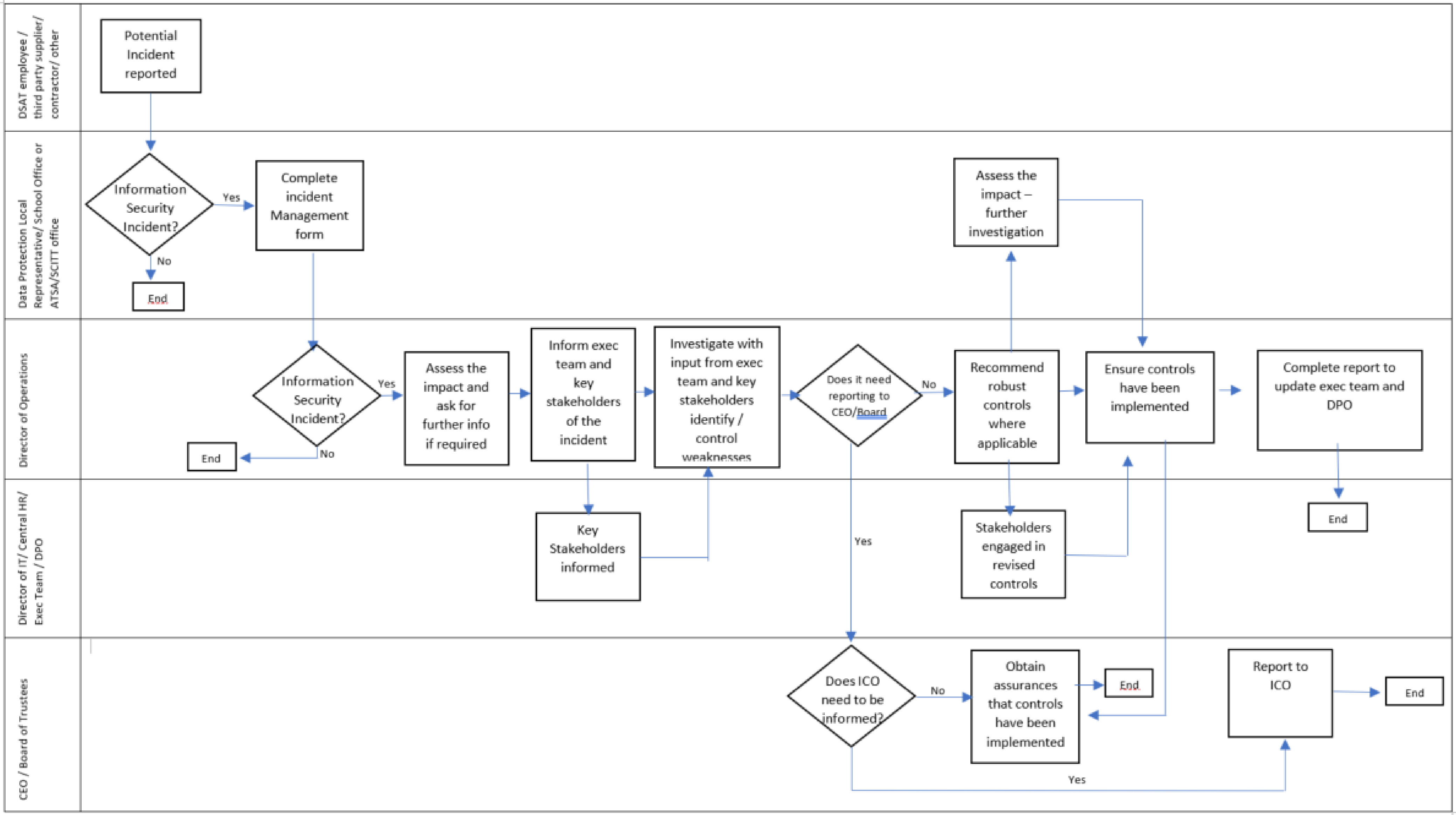
| **FURTHER ACTION: (to be completed by Director of Operations)** | |
|---|---|
| **Completed by:** | |
| **Is further action required?** | Yes/No |
| **Has the case been discussed with the Executive Team?** | Yes/No |
| **Have data subjects been informed?** | Yes/No |
| **Have key stakeholders been informed?** | Yes/No |
| **Have control weaknesses been highlighted and recommendations made?** | Yes/No |
| **Has sufficient and appropriate action been taken?** | Yes/No |
| **Does the incident need reporting to the ICO?** | Yes/No |
| **Has the Incident Log been updated?** | Yes/No |
| **Further investigation undertaken by:-** | |
| **Date incident closed:-** | |

**You can also contact the following people for advice:**

**Nathan Thirlby – Director of IT**

**Nick Layfield – DPO**

## Appendix 4: Information Security Incident Management Process diagram


DSAT employee / third party supplier/ contractor/ other
Data Protection Local Representative/ School Office or ATSA/SCITT office
Director of Operations
Director of IT/ Central HR/ Exec Team / DPO
CEO / Board of Trustees
Potential Incident reported
Information Security Incident?
Yes
No
End
Complete incident Management form
Assess the impact – further investigation
Information Security Incident?
Yes
No
End
Assess the impact and ask for further info if required
Inform exec team and key stakeholders of the incident
Investigate with input from exec team and key stakeholders identify / control weaknesses
Does it need reporting to CEO/Board
No
Recommend robust controls where applicable
Ensure controls have been implemented
Complete report to update exec team and DPO
End
Key Stakeholders informed
Yes
Stakeholders engaged in revised controls
Does ICO need to be informed?
No
Obtain assurances that controls have been implemented
End
Report to ICO
End
Yes