Inspiring Futures Through Learning

Data Breach Policy

April 2021 to April 2023

At Inspiring Futures through Learning, we are driven by our pursuit of excellence every day. We have high expectations of learning, behaviour and respect for every member of our community. We create independent, articulate thinkers and learners who have confidence in, not only their individual ambitions, but also those of the Academy and The Trust as a whole. We have collaboration at the heart of everything we do and our vision is to nurture exciting, innovative, outstanding Academies who embrace change and provide a world-class education for all it serves.

***Including all IFtL Schools, Milton Keynes Teaching School Alliance and Two Mile Ash Initial Teaching Training Partnership**

Policy name:		Data Breach Policy
Version:		V2
Date relevant from:		April 2021
Date to be reviewed:		April 2023 *This policy will be reviewed every two years unless legislation dictates otherwise. Recent changes in Legislation will need to be read and used to review this Policy.*
Role of reviewer:		IFtL Head of Operations
Statutory (Y/N):		Y
Published on website*:		3C

Policy level:**	1
Relevant to:	All employees through all IFtL schools and departments
Bodies consulted:	
Approved by:	IFtL Finance and Resources Committee
Approval date:	4th May 2021

Key:

**** Publication on website:***

IFtL website		**School website**	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

***** Policy level:***

1. Trust wide:
   - This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
     - *Approved by the IFtL Board of Trustees.*
2. Trust core values:
   - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore from the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
     - *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
     - *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*

3. School / department policies
   - These are defined independently by schools / departments as appropriate
     - *Approved by school / department governance bodies.*

Introduction

Inspiring Futures Through Learning (referred to in this policy as the MAT, the trust or IFtL) collects, holds, processes, and shares personal data on various groups including pupils, staff and visitors.

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

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

Purpose and Scope

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

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

This policy relates to all personal and special category (sensitive) data held by the MAT regardless of format.

This policy applies to all staff and students across the MAT. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the trust and all staff working in MAT schools and departments.

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.

Definitions / Types of breach

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

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 trust's information assets and / or reputation.

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

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);

equipment theft or failure;

system failure;

unauthorised use of, access to or modification of data or information systems;

attempts (failed or successful) to gain unauthorised access to information or IT system(s);

unauthorised disclosure of sensitive / confidential data;

website defacement;

hacking attack;

unforeseen circumstances such as a fire or flood which compromises or restricts access to data;

human error causing a breach;

social engineering or phishing attacks where information is extracted.

Reporting an incident

Any individual who accesses, uses or manages the trust's information is responsible for reporting data breaches and information security incidents immediately, to the Data Protection Officer (at dpo@iftl.co.uk) and directly to their own Headteacher (or to the Chair of Governors where the Headteacher is not available).
Breach reporting must be carried out using the GDPRiS system which is in place across all IFtL schools. If the individual is not able to report the breach themselves, the school's data protection lead should log the report.
The DPO will report any breaches that are considered serious to the Board of Trustees via the Head of Governance or Clerk to Trustees.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many

individuals are involved. Where photographs would help the recording or investigation of the breach, they should also be attached to the report in GDPRiS.

As a part of the reporting process, breach numbers will be reported to Trustees on a regular basis.

All staff should be aware that any breach of Data Protection legislation or of Trust policy may result in the trust's Disciplinary Procedures being instigated.

Containment and recovery

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach. The DPO will then inform the school's Headteacher or Chair of Governors where appropriate.

An initial assessment will be made by the DPO in liaison with relevant senior staff in the school to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO).

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Advice from experts within the trust, or external advisors, may be sought to help resolve the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

the type of data involved;

its sensitivity;

the protections in place (e.g. encryptions);

what has happened to the data (e.g. has it been lost or stolen);

whether the data could be put to any illegal or inappropriate use;

data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);

whether there are wider consequences to the breach.

Notification

The LIO and / or the DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them as soon as possible, and within 72 hours of becoming aware of the breach.

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

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation[1];
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal / contractual notification requirements;
- the dangers of over notifying to the ICO. Not every incident warrants notification and over notification may cause disproportionate enquiries and work (current advice from the ICO is

[1] Individual Rights: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individualrights/

to make contact by telephone initially. They can then talk through the incident and help make a decision as to whether or not it is officially notifiable).

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification 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 trust or the school for further information or to ask questions on what has occurred.

The LIO and / or the DPO must consider notifying third parties such as the police, insurers, banks 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 LIO and or the DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation and response

Once the initial incident is contained, the LIO or 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.

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 including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the board of trustees.

Prevention of Breaches

There are steps that can be taken to help prevent, or reduce the impact of data breaches. Some of these are listed here.

School should have clear naming conventions for documents to reduce the likelihood of inadvertently attaching the wrong document to an email. General file names that do not clearly identify what the file contains should be avoided.
If files are for internal use only, consider including the words 'internal only', or similar, in the document title.

Documents that contain personal data, particularly sensitive personal data, should be password protected as a matter of routine. This ensures that should any accidental distribution of the document to unauthorised persons occur, they will not be able to access the document without the password.

Schools should have a system for checking that the correct data is being sent out when documents are sent via email, or by other means. Where possible, a further check by another member of staff may be appropriate.

Schools should also ensure that all staff are aware of using BCC when sending emails to multiple recipients, particularly to parents or to persons outside the trust and that email addresses should be double checked before clicking send to ensure that the correct recipient is specified.

Further Guidance

For further guidance on data breaches, please refer to the ICO guidance at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Policy Review

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

APPENDIX 1

DATA BREACH REPORT FORM

Please note, this form has been included as a means of collating information only. Reports should no longer be filed on this form and must be logged on GDPRiS instead.

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of

Department/School immediately, complete Section 1 of this form and email it to the Data Protection Officer (dpo@iftl.co.uk)

All breaches must also be recorded on your breach log, located on the trust's Sharepoint portal

Section 1: Notification of Data Security Breach	**To be completed by Head of Dept./School of person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief 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):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach and if appropriate IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: is there a backup of the data available?	
Is the information unique? Will its loss have adverse operational, research, financial, legal liability or reputational consequences for the trust or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	

HIGH RISK personal data • **Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Personal information relating to vulnerable adults and children;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed.	
• Any information relating to safeguarding or child protection issues	
Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the IFtL Executive Team or the Board of Trustees	

Section 3: Action taken	**To be completed by Data Protection Officer and/or Lead Investigation Officer**
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and Headteacher on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Investigation Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**

Appendix 2: Data Breach: What to do