General Data Protection Regulations (UK GDPR)

Crabtree Farm Primary School

Data Incidents and Breaches Policy

May 2022

Data Incidents and Breaches

Contents

Dealing with Data Incidents and Breaches

This guide is designed to assist colleagues in dealing with and appropriately responding to data incidents.

1. Introduction

Under the General Data Protection Regulation and the Data Protection Act 2018 a personal data breach must be notified to the Information Commissioners Office (ICO), no later than 72 hours after becoming aware of a data breach (unless a breach is unlikely to result in a risk to the rights and freedoms of individuals) and in certain cases, communicate the breach to the individuals whose personal data have been affected by the breach. This policy is to be read in conjunction with the Data Protection Policy and other relevant guidance. The policy describes the procedure to be followed by members of staff when they become aware of a data breach.

2. Duty to protect personal information

The school has a duty under the sixth principle of Article 5 of the General Data Protection Regulation (GDPR) and section 33 to 38 of the likely Data Protection Act 2018 to ensure that it takes appropriate technical and organisational measures to protect the personal information it holds against unauthorised or unlawful processing, accidental loss, misuse, destruction, and damage.

Despite robust policies, guidance and procedures being in place, occurrences of data incidents involving loss or inappropriate access may still occur due to human error, wilful wrongdoing or other unforeseen circumstances. This document sets out the procedure which should be followed when a data incident occurs and the expected action(s) to be taken by:

- the person reporting an incident
- the Data Protection Officer (Melanie Smith) who will be dealing with the incident
- the Data Protection Officer who will report the matter to the ICO if it is a personal data breach

3. What is a data incident?

A **Data Incident** is a process failure where it appears personal data or information in any medium (paper, electronic, laptop, data stick, etc.), including verbal information, is:

- Sent, handed, or given verbally to someone who should not have access to it
- Lost or stolen
- Accessed inappropriately either intentionally or unintentionally
- Transmitted insecurely or uploaded inappropriately to a webpage
- Disposed of in an unsecure manner.

Examples of data breaches in school include:

- A full sickness record mistakenly sent to new employer as part of a reference
- Sensitive personal data lost in the post - about a hearing to investigate complaints about exclusion from school
- Pupil personal data found at a printer by another pupil
- Pupil reports sent to wrong address
- Email addressing - non-use of BCC where it would have been appropriate
- Text message re a pupil's behaviour intended for their parents/carers sent to all parents/carers
- Data file with staff and pupil personal data accidentally placed in shared drive
- Inappropriate disclosure of pupil's information to absent father
- Sending Special (Sensitive) Personal Data via unprotected email
- Lost unprotected USB sticks including pupil data
- Unencrypted drives / laptops / devices stolen from staff homes / cars / bags
- Parent passwords to access child information not sufficiently strong
- Poor website security; personal data left accessible by inadequate technical safeguards, e.g. inaccurate coding, inadequate penetration testing, etc.

4. When is a data incident a breach, or a near miss or no breach?

A data incident only becomes a **Data Breach** if, upon investigation by the Data Protection Officer it is found that security is breached because sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. The severity level of the data breach is determined by elements such as the number of individuals affected, the sensitivity of the information, containment of the incident, recovery of the data and assessment of on-going risk.

Investigation of a data incident can find that a **Near Miss** or **No Breach** has taken place. A **Near Miss** highlights areas at risk of data breaches, but is an event that did not actually result in a breach although it had the potential to do so. For example an encrypted email containing personal information is sent in error to a partner organisation but no personal information can be accessed; personal information sent in error to colleague or a partner organisation but it is password protected; information is lost, but recovered without any of the contents being disclosed to anyone.

An event where at first sight a data breach has occurred, but after investigation it proved not to be a breach is classed as **No Breach**, e.g.

- It was found the information was accessed legitimately

- The school is not the data controller. The controller is the body that determines the purpose and means of processing the data, e.g. if a School Nurse emailed pupils' medical details to an NHS colleague insecurely. In this case, the NHS would have authority as the data controller and would deal with the incident.

5. Reporting a data incident to the Data Protection Officer

Upon discovering a data incident staff should immediately notify the Data Protection Officer (or another senior teacher if the Data protection Officer is unavailable) and take any steps necessary to reduce the impact of the incident. The Data Protection Officer should then:

- Complete without delay the Data Incident Reporting Form to collect the facts surrounding the incident

- Take any additional steps necessary to reduce the impact of the incident - for example getting information taken down from the internet, retrieving information sent to the wrong address etc.

- Notify the ICO as soon as possible within 72 hours unless a breach is unlikely to result in a risk to the rights and freedoms of the individual.

- Where it is clear that there is a high risk to the rights of the pupil or other data subject affected, then they must also be notified, or a parent or carer for that pupil.

- Where it is unclear advice should be sought from the ICO as to whether affected individuals would need to be notified.

Any data loss or data misuse incident <u>must</u> be reported to the Data Protection Officer.

6. What is a personal data breach?

The General Data Protection Regulation describes a personal data breach as being *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.* This means that any breach of principle 6 (security) that contains personal data is likely to be a personal data breach. It is a type of security incident. However, if a complaint is made in relation to another principle this may be a breach but will not be a personal data breach.

7. When should the Information Commissioner's Office (ICO) be notified of a data breach?

When there is a risk to the rights of the individuals affected.

8. What happens if the school fails to notify the Data Controller within 72 hours?

The ICO have the power to fine the school up to 2% of their turnover.

9. When does the School become aware that the data breach has occurred?

The school becomes aware when they have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This will depend on the circumstances of the breach. In some cases, it will become relatively clear from the outset that there has been a breach. In others, it may take some time to establish if personal data has been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached and if so, take remedial action and notify the ICO if required. Examples include:

o   A parent/carer informs the school that they received a text or letter about another pupil by mistake and shows staff the text which provides evidence of the unauthorised disclosure. As the school have been presented with clear evidence of a breach there can be no doubt when the school became aware.

o   A teacher reports a loss of an unencrypted memory stick that contained personal information relating to a pupil at the school. In cases where a small, unencrypted device is lost, it is not normally possible to determine whether someone has gained unauthorised access to the data it contains. Consequently, an incident like this would need to be notified to the ICO as there is a reasonable degree of certainty that a breach has occurred and the school would become aware when the teacher first realised the memory stick was lost.

10. What information should be notified to the ICO?

a)   Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects / personal data records concerned.

b)   Inform the ICO of the Data Protection Officer's details or other contact point where more information can be obtained.

c)   Describe the likely consequences of the personal data breach.

d)   Describe the measures taken or proposed to be taken by the school to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

Flowchart - key steps for school staff reporting a data incident:

Action By		Immediate Action Required		Next Steps
Any member of staff who discovers a potential or actual data incident		Report a potential or actual data incident to a Data Protection Officer or if the DPO is unavailable a senior member of staff. If you receive a phone call: obtain the name and contact details of the person notifying us, and if possible try to collect some initial facts such as: o Is the incident on-going? o What type of information is involved? o Are the data subjects children or vulnerable adults? o How many data subjects are involved? o What is the likelihood of the information being recovered? o Who has the information been sent to? (i.e. who has seen the information?)		• Take any steps necessary to reduce the impact of the incident (e.g. telephoning the premises where information may have been lost or going to an address to retrieve information sent there in error
DPO to whom the data incident is reported		Collect the facts about the incident and enter them onto the data incident reporting form. Take any additional steps necessary to reduce the impact of the incident.		• Prepare breach response plan which focuses on protecting individuals and their data • Report the matter to the ICO if a personal data breach has occurred no later than 72 hours after becoming aware of the incident unless the breach is unlikely to result in a risk to the rights of the individual affected • Inform affected individuals if there is a high risk to the rights of the individuals.
DPO		The DPO needs to make an initial risk assessment of the data incident and consider any immediate actions to reduce and/or remediate the impact of the incident. Where a data incident also involves loss or theft of an encrypted or unencrypted device, then the incident the DPO should report the incident to the IT Support Team and liaise closely with them in trying to resolve it.		• Taking immediate actions to stop an on-going incident, e.g. telephoning the premises where the information may have been lost to find out if it has been handed in, going to a property to collect information sent there incorrectly, recalling emails sent to the incorrect email address. Asking unintended recipients of email to delete messages sent in error, including deleting it from their email trash.

Data Protection Officer		The Data Subjects will be notified when there is a high risk to the rights and freedoms of the individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data has been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals: ○ **Racial or Ethnic Origin** ○ **Political opinions, Religious or Philosophical beliefs** ○ **Trade Union Membership** ○ **Data concerning Health or Genetic Data** ○ **Data concerning Sex Life or Sexual Orientation** ○ **Criminal Conviction** **Such damage should be considered likely to occur and therefore, data subjects should be notified as a matter of course.**		• Informing data subjects of the incident, and if they are at risk due to the incident, giving clear advice on the steps they can take to protect themselves. • Informing the police where appropriate, e.g. where property is stolen, where fraudulent activity has taken place, an offence under the Computer Misuse Act or the GDPR has occurred.

Flowchart - key steps for DPOs when investigating a data incident:

Action By		Immediate Action Required		Next Steps
DPO	➡	Once the facts surrounding the incident are gathered, The DPO investigates the cause of the incident. Each case is different but it is likely that it will involve finding answers to a series of questions such as: What events led up to the incident? Had the staff involved received sufficient levels of training to prevent the incident from happening? Are there written procedures setting out the expected behaviour of staff? Were procedures setting out expected behaviour followed? Does the incident involve sub-contractors? Is there a contract or agreement in place to set out expected behaviour? Has the same type of incident happened before? Has the same type of incident happened before in the school? How widespread is the incident? Is there a chance that this has routinely happened before but only just been discovered? Are there any others?	➡	In some instances, the facts around a case may be incomplete. This may be because there was a delay in reporting the incident. Any delay past 72 hours will need to be explained to the ICO. Where the facts are incomplete, it may be necessary to answer questions such as: • Why are there gaps in the facts • Can the person (who may have left the school) be contacted in an attempt to obtain missing facts Where other organisations are involved (e.g. Police) it may be necessary to work with them to gain complete understanding of the incident. Extra efforts may be needed to try and recover lost information, such as: ○ Speaking to staff members to get their recollections of the incident ○ Searching in files in use at the same time as the lost information ○ Checking data in Capita Sims ○ Searching in waste / recycle bins ○ Searching on backup tapes Once the incident has been investigated it should be categorised. Not all reported incidents are actual data breaches. Incidents are categorised as either: ○ Data breach reportable to the ICO ○ Data Breach reportable to the ICO and the Data subjects ○ Non- reportable data breach ○ No breach If the DPO decides that the incident should be reported to the ICO, then they will draft an email covering the incident, the actions taken and any further proposed actions. The email will be sent to casework@ico.gsi.gov.uk, copying in the Headteacher and Chair of Governors. *Remember to send information securely, i.e. using encrypted e-mail software.*

Flowchart - key steps for Data Protection Officer producing an action plan to reduce the likelihood of the incident recurring:

Action By		Immediate Action Required		Next Steps
Data Protection Officer	→	Once any immediate and urgent actions have been taken and the investigation into the incident has been carried out, an action plan needs to be drawn up which is designed to reduce the likelihood of a similar incident occurring again. Every incident is different and therefore the action plan drawn up will be unique to address the set of circumstances that led up to the incident. However, across all incidents there are a number of common contributory factors that can be addressed in a similar way, e.g. changes to procedures, raising awareness, etc. A list of actions to address these more common contributory factors is set out in Appendix 1. The DPO should ensure that any contributory factors that are specific and unique to a particular incident are addressed.	→	• Details of agreed actions, deadlines, and evidence required will be kept by the DPO and any actions carried out by the relevant member of staff. • Evidence that actions have been completed should be sent by the member of staff to the DPO.

Flowchart - key steps for Data Protection Officer monitoring an Action Plan until all actions have been completed:

Action By		Immediate Action Required		Next Steps
Data Protection Officer	→	The case remains open until all actions required to: ○ remediate the effects of the incident ○ reduce the likelihood of a recurrence are completed.	→	Completion of actions will ensure the school is working as safely as possible thus reducing the risk of further incidents occurring.

Flowchart - key steps for the Data Protection Officer closing the case and reassessing on-going risk:

Action By		Immediate Action Required		Next Steps
Data Protection Officer	→	Once all actions included in the action plan have been completed and the level of on-going risk has been assessed the case can be closed.	→	An assessment should be made of the level of on-going risk. This should be carried out to determine whether the risk is the same, lower or higher than at the conclusion of the investigation into the risk of recurrence carried out three months earlier. If the risk level remains the same or is now lower, no further action needs to be taken. If the risk level is **higher** than at the previous assessment, the action plan needs to be revisited.

Appendix 1 – most frequently occurring data incidents

This table contains a list of the most frequent occurrences of data incidents, along with the remedial action to be taken and the evidence required to prove that the action has been completed.

The following advice should be provided to all school staff to remind them of the need to maintain security around personal/confidential information:

- All staff members should undertake Data Protection training at least annually.

- Ensure that personal information is kept secure: lock/turn off your screen when not in use, secure information in lockable cabinets, use passwords/encryption (e.g. Office 365 encryption, Cryptshare, etc.) to share personal information.

- Colleagues should only use school IT approved encrypted electronic devices for school business; this is particularly important if devices are mobile and taken off-site (i.e. laptops, mobile phones, etc.)

- Lockable bags should be used when colleagues need to transfer/transport hard copy information.

- Double-check your email/letter address (or have a colleague do this) before you sent it. Ensure that you have the correct address.

Data Incident	Remedial action	Evidence required
No established procedure on dealing with personal information, and/or procedure not properly documented, and/or colleagues not receiving adequate procedure training, and/or procedure not being followed.	Write procedure and train colleagues accordingly.	Copy of procedure. Email confirmation from manager that training has taken place.
Staff have not received (refresher) Data Protection training.	Undertake Data Protection training.	Copy of training certificate.
Staff knowingly, wilfully and wrongly accessed information (i.e. information not pertinent to their role, without line management approval, etc.)	Disciplinary action.	Email confirmation from line-manager that disciplinary action is being taken.

Incorrect personal information held in pupil school management information system (e.g. wrong address or phone number, email address, etc.).	Correct the information held and review the process for minimising the recording of incorrect information in the future.	Email confirmation from staff member that information has been updated and copy of new procedure sent to staff.
Information transported insecurely, e.g. pupil files carried in plain sight on the seat of car	Provide staff with lockable bag/mail pouch. Ensure that the importance of using secure bags is communicated to all staff and that it is included in the procedure transferring / transporting records.	Copy of a communication to staff. Copy of procedure.
Personal/confidential information sent by unencrypted email (or without a password). Information shared from or stored on unencrypted/non IT Approved electronic devices and/or on non IT approved Cloud storage.	Ensure that the importance of using encryption and always using only officially approved electronic devices is communicated to all staff, i.e. do not use your own mobile phone, laptop, tablet for work purposes. Ensure that it is included in an IT Acceptable Use Policy/procedure. Ask the recipient of the information to delete it and also remove it from their deleted items folder. Ensure that Cloud storage (if applicable) is deleted too.	Copy of any team meeting minutes/memo re communication to staff. Copy of procedure. Confirmation from recipient that information has been deleted.
Issues with outgoing correspondence e.g. an incorrect recipient.	Always double-check letters/emails (or have a colleague do this) before they are sent to ensure that the (email) address is correct. Always include 'private, personal, confidential' above the name and address of the recipient of a letter. Ensure that it is included in the procedure.	Copy of letter template. Copy of procedure.

Incorrect documents picked up or documents left behind on the printer/photocopier.	Wherever possible, staff should stay with the printer/photocopier whilst printing/copying is in progress and ensure that all hard copies are collected. Care should be taken that no other documents are accidentally picked up (i.e. documents left behind by another user). Ensure that it is included in the procedure.	Copy of procedure.
Devices stolen or misplaced.	Ensure the school encrypts all its computers and other devices wherever it is practicable to do. Make sure staff understand the importance of using encryption, password protection and storage devices correctly and securely. Ensure that it is included in the procedure. If a device is misplaced and later found at found e.g. at a pupils home, establish who has access to it and that it is secure whilst it awaits collection. Let IT Support and Police know of the loss/theft.	Copy of procedure. Correspondence from IT and Police.
Inappropriate discussion of confidential case details with colleagues who are not involved in the case or with other 3rd parties. Confidential case discussion in a public area or open plan office. Inappropriate discussion a case with a parent of a pupil whilst other family members/carers or other parents are also present.	Ensure that staff are aware of the importance of keeping personal information personal, and that they are aware of: o what they can and cannot share with colleagues/agencies o their surroundings when discussing a case (i.e. can they be overheard)the need to obtain the pupils/parent consent before discussing their personal information in front of their family members/carers. Undertake Data Protection training.	Copy of procedure. Copy of training certificate.

Sharing of personal/confidential information on social media or other online tools or cloud storage.	Ensure that staff are aware of the importance of keeping personal information safe and that they should not generally, use social media, online tools, cloud storage for sharing, saving, communicating personal information. Ask the person who uploaded the information to remove it from social media. Ensure that it is deleted from cloud storage too.	Copy of procedure. Confirmation from person who uploaded information that information has been deleted.
Incorrect disposal of confidential waste.	Ensure that staff are aware of the importance of disposing of all confidential waste in the confidential waste bins provided.	Copy of procedure.

Appendix 2 - Breach Log for recording data incidents

The table form below provides a simple breach log for recording data breaches. It is sourced from the Information Commissioner's Office (ICO) who require its service providers to use the form when reporting breaches.

ico.
Information Commissioner's Office

Personal data security breach log

Organisation:									Date:				

No.	Your ref.	Details of breach						Consequences of breach	Measures taken/to be taken			
		Date of breach	No. people affected	Nature of breach (choose most relevant)	Description of breach	How you became aware of breach	Description of data		All individuals informed?	Remedial action	Other Regulators informed	When did you first notify the ICO of the breach?