St Michael's CE (A)

Primary School

Data Breach Policy and Procedures

The Lord says, 'For I know the plans for you…plans to give you hope and a future.'

Jeremiah 29 verse 11

Policy adopted: Thursday 21st November 2019

Policy Review: November 2020

Signed: ***Zoe Wilson*** (Chair of Governors)

St Michael's CE (A) Primary School

Guidance: How to respond to an information incident / personal data breach

Under the General Data Protection Regulations (GDPR) a personal data breach is defined in Article 4(12) and in the Data Protection Act 2018 Chapter 1 paragraph 33 (3) 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"

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Some examples of a personal data breach include:

- Sending personal data to an incorrect recipient;
- IT devices containing personal data being lost or stolen;
- Access by an unauthorised third party;
- Alteration of personal data without permission;
- Loss of availability of personal data; and
- Deliberate or accidental action (or inaction) by a data controller or processor.

What breaches do you need to report?

GDPR / Data Protection Act 2018 makes it a requirement to inform the Information Commissioner's Office (ICO) of personal data breaches where it is likely to result in a risk to the rights and freedoms of individuals. You must do this within 72 hours of becoming aware of the breach, where feasible. In some cases, this will also mean that the controller will also have to inform the affected individuals. The ICO now has the power to take stricter enforcement action if they discover a breach that has not been self-reported.

If you believe a personal data breach has occurred, you must report it immediately or without any undue delay to the Head Teacher or Business Manager of the school or the school's Data Protection Officer on: City of Wolverhampton Council] 01902 5555166 or 01902 558653, email SchoolsIG@wolverhampton.gov.uk

All information incidents that have, or could have, a security or privacy impact should be recorded. Records are maintained to manage these incidents and to look for trends so that preventative measures can be taken. Far more is recorded than is required to be reported to the ICO. This is because it is necessary to maintain a record of the decision making process justifying why you do not need to report the breach. Many of these incidents will not be data breaches as such, but without a clear definition of what a breach is it is not possible to be objective and consistent. This in turn could lead to over reporting, which is unsustainable, or under reporting which would not be compliant with GDPR / Data Protection Act 2018.

- Practical considerations:

In practice there are three levels of occurrence that we need to define. These are:

- Events;
- Incidents; and
- Breaches.

- What is an event and when does an event become an incident or a data breach?

Events happen all the time, they are non-routine occurrences that are worthy of note, but may not need to be taken any further as they can be managed locally.

Type of Occurrence	What does this mean	How is it dealt with
Event	Something unexpected happened involving personal information or data systems.	Employees or, where necessary, management of the business area where it happened deal with it unless it meets the criteria to become an incident or breach. Employees should seek advice from school's Head Teacher or Business Manager or the school's Data Protection Officer to decide this if they are uncertain.

Some events will turn out to be **incidents** that need to be reported internally using the Information Event/Incident - Initial Assessment and Reporting Form (see Appendix 1).

Type of Occurrence	What does this mean	How is it dealt with
Incident	An event that has, or could have an undesirable consequence on the confidentiality, integrity and/or availability of personal information with the potential to impact upon the information rights of individual(s).	Needs to be reported to the school's Head Teacher or Business Manager and the school's DPO It must be recorded and assessed to see if a breach has occurred that requires reporting to the ICO; Assessed to see if appropriate containment and corrective action to mitigate any information risks is in place; Relevant management roles informed.

Example:
You send a document that contains sensitive personal information to the printer but when you go to print it, it is not in the print queue or the document appears to have finished printing but when you return to your desk you find the document is not complete or you get distracted and leave the document on the printer.

This could be for several reasons, such as:

- It is a large document and takes time to be included in the print queue;

- It is a large document and the printer pauses before starting to print the remainder of the document and you do not realise this has happened;
- The printer runs out of paper or develops a fault and you do not fix the problem;
- You have printed multiple copies of the same document and loose count.

The first reason is an event, it's something unexpected and undesirable but can be handled locally by the employee and does not need to be reported to the Head Teacher or DPO The other reasons are more serious and will require some degree of investigation as they could impact upon the information rights of the individual(s) whose information has been potentially exposed to unauthorised access. These are incidents. Remember that information security involves maintaining the confidentiality, integrity and availability (CIA) of personal information and anything that impacts on one or more of these factors is an information incident.

Dealing with these as incidents means that the Head Teacher/Business Manager and/or the school's DPO can review what caused them, check if they are happening regularly and work with management to develop processes and procedures that can reduce the risk of reoccurrence. For example, in these cases issuing reminders to employees and placing reminder notices on printers to ensure all documents are collected.

What constitutes a data breach?

A data breach is an incident where one or more of the factors listed in the table below are significant enough to consider. Some incidents will meet the criteria for a breach and must be reported to the ICO and the data subject. As can be seen from the table this is where damage or potential damage can cause harm to an individual.

Type of Occurrence	What does this mean	How is it dealt with
Data Breach	The consequences did or could have been severe enough to result in some damage to any individual such as: • Harming their privacy and confidentiality; • Misuse or leakage of information about them; • Prevent them exercising their rights; • Lead to damage such as discrimination, identity theft, fraud or financial loss; • Defeat controls intended to protect privacy; • Damage their reputation or other social disadvantage. • Put their personal safety or liberty at risk.	These must be reported to the ICO within 72 hours of occurrence in addition to the actions for any other incident. Will often need to be reported to the data subject(s) involved in the breach. It may also need to be reported to other external bodies such as the Health and Social Care Information Centre (HSCIC), the Department of Work and Pensions (DWP) and HM Revenue and Customs (HMRC), etc., if relevant information is involved. You should seek advice from the school's Data Protection Officer if you are not sure.

This is a wide scope and we need to be consistent in how we apply this definition, not only internally but from one organisation to another. Over time, as case law develops, this will become clearer. Until then we need to look at each element of the definition and decide if it applies to the incident we are dealing with. This can be considered as a series of questions.

In the example above if the document had been left on the printer we need to consider the questions below to determine whether to report the incident to the DPO :

No.	Question	Yes	No
1	Was personal data involved in the incident	✓	
2	Was ANY loss of control over data/limitation of rights/reputational damage/social or economic disadvantage caused or likely to be caused as a result of the incident		✓
If No to either of the above then incident is not reportable. A record of the rationale behind these answers must be entered below.			
3	Explain the rationale behind any "**No**" answers to questions 1 or 2:		
2. No damage likely because the document did not contain any personal information and was an extract of a publicly available document.			
Answer YES to the questions below only if it would be reasonable to consider harm/damage could be caused			
4	Did / could anyone's privacy or confidentiality suffer?		
5	Was information about the subject misused or inappropriately disclosed?		
6	Was there or could there be an impact on the subjects' ability to exercise their rights?		
7	Is discrimination, identity theft, fraud, financial loss or similar harm likely?		
8	Were privacy measures overridden, such as pseudonymisation or encryption?		
9	Did / could the subject suffer reputational damage or other social harm?		
*If you answer "**Yes**" to any question in the section above the incident is reportable. Please provide a note for each question (4-9) you have answered Yes to in the box below.*			
10	Add any further justification for the answers for any of the questions above:		

Sample answers are shown in green to distinguish them from the template.

Incident review and investigation

Note that the above table is used only to decide whether to report the incident, it does not replace the details which need to be captured as part of the investigation. The initial review of the situation, must be

carried out quickly as it will provide the details necessary to answer the questions in the table. Where it is determined that an incident has occurred you must report it to the DPO, immediately. It is important to note that if the incident is a breach, it must be reported to the ICO within 72 hours of the incident occurring. Organisations can be fined for not meeting this deadline or for failing to report, even if the incident itself does not warrant a fine. Other details about the incident will need to be recorded as we need to ensure all relevant details are available for external reporting. The standard Information Incident Reporting Form, see Appendix 2, is used for this.

As a further example, let's look at an email sent to an unintended recipient. In this example a letter being sent as an email attachment inviting a parent to attend a meeting has been sent to another parent who has a similar name to the intended recipient that was accidently selected from the list of email addresses that appeared when typing in the first few letters of the person's name in the 'To' box. The unintended recipient immediately replied stating that the letter was not for them and that they had deleted the email.

In this case the assessment would look like this:

No.	Question	Yes	No
1	Was personal data involved in the incident	✓	
2	Was ANY loss of control over data/limitation of rights/reputational damage/social or economic disadvantage caused or likely to be caused as a result of the incident	✓	
If No to either of the above then incident is not reportable. A record of the rationale behind these answers must be entered below.			
3	Explain the rationale behind any "**No**" answers to questions 1 or 2:		
Answer YES to the questions below only if it would be reasonable to consider harm would be caused			
4	Did / could anyone's privacy or confidentiality suffer?	✓	
5	Was information about the subject misused or inappropriately disclosed?	✓	
6	Was there or could there be an impact on the subjects' ability to exercise their rights?		✓
7	Is discrimination, identity theft, fraud, financial loss or similar harm likely?		✓
8	Were privacy measures overridden, such as pseudonymisation or encryption?		✓
9	Did / could the subject suffer reputational damage or other social harm?		✓
*If you answer "**Yes**" to any question in the section above the incident is reportable. Please provide a note for each question (4-9) you have answered Yes to in the box below.*			
4. The information was viewed by the unintended recipient and they are aware of the name and address of the parent but no other personal information was contained in the letter 5. The information was inappropriately disclosed due to human error. On this occasion the data breach was quickly contained and the unintended recipient did not intend to make a complaint.			
10	Add any further justification for the answers for any of the questions above:		

In this case the incident is reportable, even though it was contained in a short time.

Grading of Information Incidents

Any incident will be graded according to the impact of the breach and the likelihood of serious consequences occurring. The incident will be graded according to the impact on the individual or groups of individuals.

The impact is graded rating the incident on a scale of 1-5. 1 being the lowest and 5 the highest.

The likelihood of the consequences occurring are graded on a scale of 1-5. 1 being a non-occurrence and 5 indicating that it has occurred.

Where the personal data breach relates to a vulnerable child the minimum likelihood grading will be 2 even if no adverse effect occurred.

Grading of incidents will be reviewed by the Head Teacher/Business Manager and the Data Protection Officer when determining what the impact and likelihood a data breach will be.

Breach Assessment Grid:

This operates on a 5 x 5 basis with anything other than “green breaches” being reportable.

Impact	Catastrophic	5	5	10	15	20	25
	Serious	4	4	An impact is unlikely 4	Reportable to ICO and Data Subject(S) 8	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	Reportable to the ICO and consider notifying Data Subjects 6	8	10
	No Impact	1	1	2	3	4	5
			No Impact has occurred				
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood harm has occurred				

Further Guidance

The ICO have produced a guide on GDPR and Personal data breaches.

Appendix 1

Information Event/Incident - Initial Assessment and Reporting Form

This form is for any council employee to complete when reporting an information incident. It should not take more than 5 minutes to complete.

If you are unsure about the procedures for reporting an information incident, you should read the school's guidance 'How to respond to a personal data breach'.

Please provide as much information as possible.

Description of the information event/incident

Please describe the event/incident in as much detail as possible.	
When did the event/incident happen?	
How did the event/incident happen?	
How were you made aware of the event/incident?	
Has the event/incident been contained in any way? If Yes, please detail.	

Initial assessment of the information event/incident

No.	Question	Yes	No
1	Was personal data involved in the incident		
2	Was ANY loss of control over data/limitation of rights/reputational damage/social or economic disadvantage caused or likely to be caused as a result of the incident		
If No to either of the above then incident is not reportable. A record of the rationale behind these answers must be entered below.			
3	Explain the rationale behind any "**No**" answers to questions 1 or 2:		
Answer YES to the questions below only if it would be reasonable to consider harm would be caused			
4	Did / could anyone's privacy or confidentiality suffer?		
5	Was information about the subject misused or inappropriately disclosed?		
6	Was there or could there be an impact on the subjects' ability to exercise their rights?		
7	Is discrimination, identity theft, fraud, financial loss or similar harm likely?		
8	Were privacy measures overridden, such as pseudonymisation or encryption?		
9	Did / could the subject suffer reputational damage or other social harm?		
*If you answer "**Yes**" to any question in the section above the incident is reportable. Please provide a note for each question (4-9) you have answered Yes to in the box below.*			

10	Add any further justification for the answers you have provided for any of the questions above:

Contact Details

Please provide your contact details should we require further information concerning the incident	
Contact Details of deputy (in case of absence)	

Sending this form

Your submitted form will be sent to the Data Protection Officer . Once received, the DPO will contact you to confirm receipt and to advise you of any next steps.

Appendix 2

Information Incident Report Form

This form is for managers and/or senior managers to complete, following the initial report of an information incident. It should not take more than 15 minutes to complete.

If you are unsure about the procedures for managing an information incident, you should read the School's Information Incident Policy.

Please provide as much information as possible. If you do not know the answer or you are waiting on the completion of further enquiries please state this and indicate when this information may be available. In addition to completing the form below, please provide any other supporting information that maybe relevant.

In the wake of an information incident, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals and the School, and details of the steps taken to achieve this should be included in this form.

Contact Details

Please provide your contact details should we require further information concerning the incident (Name and job title, email address and contact telephone number)	

Details of the information incident

Please describe the incident in as much detail as possible.	
When did the incident happen?	
How did the incident happen?	
If there has been a delay in reporting the incident to the DPO, please explain your reason(s) for this.	
What measures and operational controls were in place to prevent and/or detect an incident of this nature occurring?	

Personal data placed at risk

What, if any, personal data has been placed at risk? Please specify if any financial, commercial or personal sensitive data has been affected and provide details of the extent.	
How many individuals have been affected?	
Have the affected individuals been made aware that an incident has occurred?	
What are the potential risks, consequences and adverse effects on those individuals? Loss of control over data? Limitation of their legal rights?	

Reputational damage? Social or economic disadvantages including physical harm?	
Have any of the affected individuals complained about the incident and if so, what action has been taken?	

Containment and Recovery

Has any action been taken to minimise/mitigate the effect on the affected individual(s)? If so, please provide details.	
Has the information placed at risk now been recovered? If so, please provide details of how and when this occurred.	
Have any steps been taken to prevent a recurrence of this incident? If so, please provide details.	
Who have you informed about the incident, both internal and external? For example, in the event of theft, have the Police been informed and do you have a crime number?	

Training and guidance

Please confirm that all employees involved with the incident have successfully completed data protection training?	
Has any additional Information Governance training been provided? If so, please provide details.	
Has any specific detailed operational guidance been developed and provided to staff on handling information, including the use of IT equipment? If so, please provide details.	

Previous information incidents

Have you reported any previous information incidents in the last year?	
If the answer is yes, please provide brief details.	

Investigation

Have you asked any questions to determine the circumstances leading to the loss of information? If so, please provide details.	
What, if any actions have been taken to preserve evidence and/or create an audit trail relating to the information incident?	

What, if any, remedial actions have been taken since the information incident occurred to prevent any recurrence?	
Where remedial actions have been identified what timescales have been agreed for their implementation? Please provide details.	

Sending this form

Send your completed form and any related attachments within 1 day of the date of the incident to:

Your designated Data Protection Officer:

City of Wolverhampton Council 01902 5555166 or 01902 558653, email SchoolsIG@wolverhampton.gov.uk

What happens next?

When the DPO receives this form, they will contact you to provide:

- An incident reference number; and
- Information about our next steps

If you need any help in completing this form, please contact SchoolsIG@wolverhampton.gov.uk or Martin Eades, Senior Information Governance Officer, City of Wolverhampton Council, Telephone number: 01902 558653.

Information Governance Team Use Only:	
WCC Incident Reference Number	
Impact / Likelihood Score	
Notify the ICO (Grading result score amber / red)	Yes / No
Notify the Data Subject(s) (Grading result score 8 or above amber / red)	Yes / No

Flow chart showing assessment/notification requirements