Thirsk Community Primary School
Information Security Incident Reporting Policy

Introduction

This policy has been written to govern the **Thirsk Community Primary School** management of information security incidents and data breaches.
Queries about any aspect of **Thirsk Community Primary School** Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at SchoolsDPO@veritau.co.uk

Scope

This policy applies to all **Thirsk Community Primary School**'s employees, any authorised agents working on behalf of the school, including temporary or agency employees, governors, and third-party contractors. Individuals who are found to infringe this policy knowingly or recklessly may face disciplinary action.

The policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Article 33 of the UK GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer; and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s). Therefore, it is vital that the **Thirsk Community Primary School** has a robust system in place to manage, contain, and report such incidents. The Information Security Incident Management Policy details how the **Thirsk Community Primary School** will handle and manage information security incidents when they arise.

Notification and Containment

In order for the **Thirsk Community Primary School** to report serious incidents to the ICO within 72 hours it is vital that it has a robust system in place to manage, contain, and report such incidents.

Roles and Responsibilities

Single Point of Contact – Headteacher Mr Richard Chandler
Senior Information Risk Owner (SIRO) – Mr R Chandler
Information Asset Owner (IAO) – as detailed in the Information Asset Register
DPO – Veritau

Immediate Actions (Within 24 Hours)

If an employee, governor, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and

the **Specific Point of Contact (SPOC)** within 24 hours. If the **SPOC** is not at work at the time of the notification, their nominate deputy would need to start the investigation process.

If the breach has the potential to have serious or wide-reaching detriment to data subjects, then the Data Protection Officer **must** be contacted within this 24-hour period.

If appropriate, the individual who discovered the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Assigning Investigation (Within 48 Hours)

Once received, the **SPOC** will assess the data protection risks and assign a severity rating according to the identified risks and mitigations using the risk matrix (appendix one). An investigation report should be completed (appendix two).

The **SPOC** will notify the **Senior Information Risk Owner (SIRO)** and the relevant **Information Asset Owner (IAO)** that the breach has taken place. The **SPOC** will recommend immediate actions that need to take place to contain the incident.

The **IAO** will assign an officer to investigate near misses, Very Low, Low and Moderate incidents. High or Very High incidents will be investigated by the **Data Protection Officer** with the assistance of Internal Audit and Counter Fraud Teams if appropriate.

Reporting to the ICO/Data Subjects (Within 72 Hours)

The **SIRO**, in conjunction with the relevant manager, **SPOC**, **IAO** and **DPO** will decide as to whether the incident needs to be reporting to the ICO, and whether any data subjects need to be informed. The **relevant manager/IAO** will be responsible for liaising with data subjects and the **DPO** for liaising with the ICO.

Investigating and Concluding Incidents

The **SPOC** will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the **DPO** has investigated a data breach then the **SIRO** must sign off the investigation report and ensure recommendations are implemented across the **Thirsk Community Primary School**.

The **SIRO** will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

All incidences should be recorded on the **Thirsk Community Primary School** breach log, along with the outcome of the investigation.

DPO Contact details:

Schools Data Protection Officer

Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01904 554025

Please ensure you include the name of your school in all correspondence

Appendix One

Risk Assessment Matrix

This matrix is designed to help you assess the risk associated with a data breach. Following a breach, please complete the steps below by ticking the boxes that apply.

You should provide the risk score and rating to Veritau when you report the breach.

If you need assistance with any aspect of this process, please contact our helpline.

Step 1

How many individuals' personal information is at risk?	Number of data subjects affected	Score	Selection
	0-10	+0	☐
	11 -50	+1	☐
	51-100	+2	☐
	101 -500	+3	☐
	500 -1000	+4	☐
	1000 or more	+5	☐

Step 2

Sensitivity factors – select each that apply		Score	Selection
Low	Contained no sensitive or confidential personal data.	-1	☐
	The information is already easily accessible or in the public domain, or it would have been published or released under FOI anyway.	-1	☐
	The information is encrypted, and it is therefore unlikely to be viewed.	-1	☐
	It was only disclosed internally, to a trusted professional who is bound by a code of confidentiality and has no personal relationship with the data subject.	-2	☐
	It was disclosed to an external trusted professional (e.g. a doctor or social worker) who is bound by a code of confidentiality and has no personal relationship with the data subject.	-1	☐
	Individuals identified are in different geographical locations or are unlikely to be known to each other and/or the recipient of the data.	-1	☐
	The information is unlikely to actually identify any individual(s).	-1	☐
High	Breach involves detailed profile information, e.g. work/school performance, salaries or personal life including social media activity, even if no special category data is involved.	+1	☐
	Breach involves high risk confidential information e.g. SEND case or safeguarding notes, spreadsheets of marks or grades obtained, information about individual student discipline or sensitive disclosures.	+1	☐

Sensitivity factors – select each that apply		Score	Selection
	The individuals affected are already known to be vulnerable, e.g. victims of a harassment or crime, a child or family under social service support.	+1	☐
	The individuals affected are likely to be placed at risk of physical harm.	+1	☐
	Wider consequences are envisaged, e.g. embarrassment to the individual, reputational damage or similar effects. They may withdraw from engaging with the school and other professionals.	+1	☐
	The incident is likely to attract media interest and/or a complaint has been made directly by a member of the public, another organisation or external individual.	+1	☐
	The incident is due to a failure to implement, enforce or follow appropriate organisational or technical safeguards to protect the information.	+1	☐
	There have been one or more previous incidents of a similar type in the last 12 months.	+1	☐
	The breach was a result of targeted malicious/criminal activity such as physical theft or a cyber attack.	+2	☐

Step 3

Effect of the breach on individuals (select one)		Score	Selection
No negative effects	There is absolute certainty that no negative effects will arise from the breach.	+0	☐
Low	Individuals are unaffected or may experience a few inconveniencies, which they will overcome easily (e.g. time spent re-entering information/changing passwords, annoyances or irritations).	+1	☐
Medium	Individuals may encounter inconveniences, which they will be able to overcome despite a few difficulties (e.g. inability to access business services, lack of understanding or stress).	+2	☐
High	Individuals may encounter significant consequences, which they should be able to overcome but with difficulties (e.g. recoverable or minor financial loss, property damage, factors affecting employment, health issues; risk of harassment, bullying or violence).	+3	☐
Very high	Individuals may encounter significant or even irreversible consequences, which they may not overcome (e.g. substantial debt or inability to work, loss of employment, long-term psychological or physical ill health, death or death threats).	+4	☐

Step 4

Likelihood that negative effects will occur (select one)			
Likelihood	**Description**	**Score**	**Selection**
Will not occur	There is absolute certainty of no negative effects. This rarely applies, and never applies to breaches involving vulnerable groups. If using this, provide evidence.	-2	☐
Not likely	There is a small possibility of a negative effect, but no evidence to rule out negative effects altogether.	+1	☐
Likely	It is fairly likely that a negative effect could occur as a result of the breach.	+2	☐
Highly likely	There is reasonable certainty that a negative effect will occur either shortly or at some point in the future.	+3	☐
Occurred	The negative effect arising from the breach has already occurred and is known.	+4	☐

Step 5

This step is only relevant if an employee obtained, accessed, edited or destroyed data when they do not have authorisation to do so.

If this is step not relevant, please continue to the next section.

Staff actions and behaviour			
Factor	**Description**	**Score**	**Selection**
Intentional	The individual was not authorised to view the information but deliberately opened or searched for the data.	+3	☐
Accidental	The individual was not authorised to view the information, but accidentally opened the data in the course of their duties.	+1	☐
No pre-existing knowledge of or relationship	The employee does not know the data subject(s) through their work or personal life.	+0	☐
Pre-existing knowledge of or relationship	The employee knows the data subject(s) either through their work or personal life.	+2	☐

Step 6: risk scoring and rating

Please calculate the total from all the steps above, and record the risk score:

Risk Score	

Based on the score you calculated, use the table below to identify the risk rating for the incident.

Score	Risk Rating
< 2 (including < 0)	Very Low
3-5	Low
6-8	Moderate
9-10	High
11+	Very High

This risk rating should be provided to Veritau when reporting the breach.

Step 7: reporting to individuals and ICO

Below is a table of the suggested reporting requirements indicated for each risk rating.

Risk Rating	Reportable to Individuals*	Reportable to ICO
Very Low	No	No
Low	No	No
Moderate	No	No
High	No	Yes
Very High	Yes	Yes

*There can be other factors to consider when reporting to individuals. Please see the additional guidance document and refer to Veritau for advice.

Appendix two

Information Security Incident Reporting and Investigation Form

Do not provide personal details of those involved or affected by a data breach. E.g. refer to them as pupils, service users, parents etc.

Stage 1: Initial recording and reporting of the incident

Serious breaches should be reported to Veritau within 24 hours of discovery.

You should use this report to record your breach in full. This is available on the Schools Portal and Veritau can assist with completing it.

Parts 1 and 2 of this report form the part of Veritau's "report a breach" function on the portal. So if you have used that function to report a breach to Veritau, you will have already completed these parts and your answers can just be pasted in to the relevant boxes below. You will then need to complete the rest of the boxes in this report to ensure the school has a full record of the breach and all actions taken.

Part 1 - About the incident	
Date and time the incident occurred	
Date and time the school became aware of the incident	
How did you first become aware of the incident? (e.g. reported by a staff member, parent or pupil)	
Who has the incident been reported to? (name and position at the school, or external organisations such as your IT team or the police)	
Incident reference number (if applicable for your school)	
Description of the incident Please provide as much detail and write as clearly as possible, including: • Who was involved and advised (job titles) • The cause of the breach (e.g. high workload, distracting workspace, new system, lack of training) • Explanation of any delay in reporting the incident	
Initial response by the school Provide details of any immediate actions that you have taken (e.g. removed published data, requested deletion of an email, password changes on systems, theft of equipment reported to the police).	
Have you been able to recover the personal data (if applicable)? Provide details e.g. you have retrieved a letter sent to the wrong parent etc.	
Have you informed the data subject(s)?	

Part 1 - About the incident	
This is the person the information relates to. If you have informed them please briefly describe their reaction (e.g. are they very concerned? Did they express any particular worries?).	

Part 2 – About the personal data	
How many individuals did the breached data relate to?	
Are there other people who may also be affected by the breach of the personal data? If so, how many? (E.g. parents of the pupils, family of a teacher etc.?)	
Categories of individuals affected Select all that apply	Employees ☐ Pupils ☐ Parents ☐ Other (please give details below): ☐ Click or tap here to enter text.
Does the information disclosed contain data that could identify the individuals? Select all those that apply	Name ☐ DOB ☐ Contact details ☐ Location data ☐ Online identifiers such as IP address and cookie identifiers ☐ Identification data such as usernames or passwords ☐ Official documents (e.g. passport) ☐ Free school meal status ☐ Other (please give details below): ☐ Click or tap here to enter text.
Does the data contain any sensitive or special category data? Select all that apply	Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Genetic data ☐ Biometric data ☐ Health data (including SEN info) ☐ Data regarding sex life or orientation ☐ Criminal offence data ☐ Safeguarding information ☐ Financial information (bank details, credit card numbers, any information indicating financial status) ☐
Are there any other details which should be noted? e.g. any additional risks which could increase the harm/detriment to individuals	

Part 2 – About the personal data	
involved or affect the investigation in any way.	

Stage 2: Risk assessment scoring

Please use the risk matrix scoring form and add the score and risk level to the box below.

Risk Score from Matrix (totals from all tables)	

Decision to inform data subjects/individuals affected

Reportable to individuals from the Matrix? Please select.	**NO**
Are there additional factors to consider regarding notifying individuals? Provide your reasoning and if specialist advice was required.	
Final decision to inform	Choose an item.
Decision makers details	
Date	Click or tap to enter a date.

Decision to inform ICO (made in conjunction with the DPO)

Reportable to ICO from the matrix? Please select.	**NO**
Are there additional factors to consider regarding notification? Provide your reasoning and if specialist advice was required.	
Final decision to inform	Choose an item.
Decision makers details	
Date	Click or tap to enter a date.
DPO details	
Date	Click or tap to enter a date.

Stage 3: Investigation

Understanding what data security measures are currently in place This section is about the internal controls that the school has in place to protect all data it holds across its systems, both electronically and physical files.	
Provide details of any relevant measures you already had in place to prevent a breach of this type occurring. For example: • Details of staff training, • What policies , processes and procedures are used within the school • Security controls in place (both physical – locked storage etc. and	

technical – passwords, encryption etc.).	
Are there relevant policies, procedures or guidance that set out what should have happened. If so what are they?	
Were the above appropriate security guidelines being followed? If not explain why.	
Has this type of incident occurred at the school before? If so, provide please a brief summary of • The date when it happened, • Who was involved in the incident (job titles) What the outcome of the investigation was (E.g. was any additional security or training put in place?)	

Training and communication This section is about whether staff understood what organisational and technical data security measures were in place	
If a member of staff was involved in the personal data breach, have they received data protection training within the last two years? (Please confirm what training has been completed)	
What evidence is there to communicate the process to be followed? (E.g. email reminders or staff meeting discussions)	
Was the training/communications provided being followed? If not explain why.	

Other factors for consideration	
Please provide any other factors that should be taken into consideration relating to the security incident. (E.g. the use of autocomplete for email addresses meant the wrong email address was selected)	
What was the root cause? (E.g. a change in working conditions, working from home, higher workload, staff absence, a lack of appropriate equipment, technology issues, lack of secure storage)	

Action Plan

This section is where you identify any improvements to reduce the risk of reoccurrence. This is also the place to record how lessons learned can be shared with colleagues. You can attach any documentary evidence to support the actions to this incident report.

	Identified area for improvement	Action required	By whom?	Date completed
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				