Information Security Incident Reporting Policy

1.0 Introduction

From May 2018 the UK's existing Data Protection Act will be replaced by the EU's General Data Protection Regulation and the Data Protection Act 2018. As part of Simonside Primary School's preparation for this new legislation, a new information policy has been developed.

This policy has been written to inform Simonside Primary School's employees what to do if they discover an information security incident.

Queries about any aspect of Simonside Primary School's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at SchoolsDPO@veritau.co.uk

2.0 Scope

This policy applies to all Simonside Primary School's employees, any authorised agents working on behalf of Simonside Primary School's including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply 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.

3.0 Notification and Containment

Article 33 of the GDPR compels data controllers to report breaches of personal data, to the Information Commissioner's Officer, within 72 hours of discovery, if the incident is likely to result in a risk to the rights and freedoms of data subjects. Therefore it is vital that Simonside Primary School's has a robust system in place to manage, contain, and report such incidents.

3.1 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)/Business Manager within 24 hours. If the

SPOC/Business Manager is not at work at the time of the notification then their Out of Office email will nominate another individual to start the investigation process.

If appropriate, the officer who located 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.

3.2 Assigning Investigation (Within 48 Hours)

Once received, the SPOC/Business Manager will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

WHITE	Information security event No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future.
GREEN	Minimal Impact A data breach has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary.
AMBER	Moderate Impact Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office.
RED	Serious Impact A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required.

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

The IAO will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams.

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

The SIRO, in conjunction with the service manager, SPOC/Business Manager, IAO and DPO will make a decision as to whether the incident needs to be reporting to the ICO, and also whether any data subjects need to be informed. The service manager/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

4.0 Investigating and Concluding Incidents

The SPOC/Business Manager 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 Council.

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