SPECIALIST EDUCATION SERVICES

Personal Data Breach Response And Notification Policy And Practice

Date created or revised: 1025
Date of next review: 0926

SES Avocet House Ltd (4926028), SES Turnstone House Ltd (7972485) and SES Kite Ltd (12634002) are subsidiary companies of Specialist Education Services Topco Ltd (13159680)

CONTENTS

1	**PURPOSE**	3
2	**SCOPE**	3
3	**RESPONSIBILITY**	3
4	**DEFINITION**	3
5	**REPORTING AN INCIDENT**	4
6	**NEXT STEPS**	4
7	**PROCEDURE – BREACH NOTIFICATION PROCESSOR TO CONTROLLER**	5
8	**PROCEDURE – BREACH NOTIFICATION: CONTROLLER TO SUPERVISORY AUTHORITY**	5
9	**PROCEDURE – BREACH NOTIFICATION: CONTROLLER TO DATA SUBJECT**	6
10	**DOCUMENTATION REQUIREMENTS**	6
11	**EVALUATION**	7
12	**SES KITE OPERATIONAL DIFFERENCES**	**7**

1 PURPOSE

Specialist Education Services ("we"/"us") have this procedure in place to provide a standardised response to any reported data breach incident and to ensure that data breaches are appropriately logged and managed in accordance with data protection law and best practice.

2 SCOPE

This procedure applies in the event of a personal data breach and applies to all employees of Specialist Education Services at all times whether located within the physical offices or not.

The document applies to all information we process, and all information technology systems utilised by us.

3 RESPONSIBILITY

All employees, contractors or temporary employees and third parties working for or on behalf of us are required to be aware of, and to follow this procedure in the event of a personal data breach.

All employees, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Manager or Data Protection Officer using the contact details as follows:

Principal Avocet House
Telephone: 01508 549320
Email: office@specialisteducation.co.uk

Principal Turnstone House
Telephone: 01508 517000
Email: office@specialisteducation.co.uk

Data Protection Officer
DPO@priviness.eu

4 DEFINITION

The GDPR defines a "personal data breach" in Article 4(12) 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". Examples include:

- Loss or theft of data or equipment on which data is stored
- Access by an unauthorised third party

- Sending personal data to an incorrect recipient
- Alteration of personal data without permission
- Loss of availability of personal data such as equipment failure
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit.
- Any unlawful processing

For the purposes of this procedure data security breaches include both confirmed and suspected incidents.

If you suspect a data breach or are unsure whether the incident which has occurred constitutes a data breach please refer the matter to the Data Manager for consideration

5 REPORTING AN INCIDENT

Any individual who accesses, uses or manages information within our organisation is responsible for reporting data breach and information security incidents immediately to the Data Manager.

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

The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information, and how many individuals are involved.

6 NEXT STEPS

The Data Manager 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 Data Manager may delegate responsibility to investigate the breach and oversee subsequent procedures to the SES Data Protection Officer.

An initial assessment will be made by the Data Manager in liaison with relevant persons (which may include IT services) to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach).

An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered or reported.

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

The Data Manager will then establish whether there is anything that can be done to

recover any losses and limit the damage the breach could cause.

The Data Manager will identify who may need to be notified. The relevant procedures from those identified below will then be followed. Every incident will be assessed on a case by case basis.

7 PROCEDURE – BREACH NOTIFICATION PROCESSOR TO CONTROLLER

Specialist Education Services must report any personal data breach or security incident to the controller without undue delay. These contact details are recorded in the Breach Register**.** Specialist Education Services provides the controller with all of the details of the breach.

The breach notification should be made by email and/or phone call.

A confirmation of receipt of this information should be requested and made by email and/or phone call.

8 PROCEDURE – BREACH NOTIFICATION: CONTROLLER TO SUPERVISORY AUTHORITY

The Data Manager will determine if the supervisory authority (the Information Commissioner's Office (ICO in the UK) need to be notified in the event of a breach.

If the breach affects individuals in different EU countries, the ICO may not be the lead supervisory authority. The Data Manager will also need to establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.

The Data Manager will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting an investigation or an impact assessment. If the Data Manager decides that there is no requirement to report the breach to the ICO the Data Manager will justify and document their decision.

If a risk to data subject(s) is likely, the Data Manager will report the personal data breach to the ICO without undue delay, and not later than 72 hours after becoming aware of it.

If the data breach notification to the ICO is not made within 72 hours, the Data Manager will submit notification electronically with a justification for the delay.

If it is not possible to provide all of the necessary information at the same time we will provide the information in phases without undue further delay.

The following information needs to be provided to the supervisory authority:

- A description of the nature of the breach.
- The categories of personal data affected.

- Name and contact details of the Data Manager.
- Likely consequences of the breach.
- Any measures taken to address the breach.
- Any information relating to the data breach.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.

The breach notification should be made via telephone - **ICO: 0303 123 1113.** Alternatively, the Data Manager may choose to report it online if they are still investigating and will be able to provide more information at a later date or if they are confident that the breach has been dealt with appropriately.

In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

9 PROCEDURE – BREACH NOTIFICATION: CONTROLLER TO DATA SUBJECT

If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Specialist Education Services will notify the data subjects affected without undue delay and in accordance with the Data Manager's recommendation.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. In any event the Data Manager will document their decision-making process.

The Data Manager will describe the breach in clear and plain language, in addition to information specified to the supervisory authority.

The controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.

If the breach affects a high volume of data subjects and personal data records, we will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder our ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner and will be considered by the Data Manager whose decision will be final.

If we have not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Specialist Education Services will communicate the data breach to the data subject(s) by telephone or email.

We will document any personal data breach within the Data Breach Register, incorporating the facts relating to the personal data breach, its effects and the remedial action taken.

10 DOCUMENTATION REQUIREMENTS

Internal breach register: there is an obligation for us to document each incident "comprising the facts relating to the personal data breach, its effects and the remedial action taken".

11 EVALUATION

Once the initial incident is contained, the Data Manager will carry out a full review of the causes of the breach; the effectiveness of the response 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 various points, including but not limited to:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks are, and identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary Identifying weak points within existing security measures
- Staff awareness

12 SES KITE OPERATIONAL DIFFERENCES

This policy applies to all SES Kiet provisions. A couple of key additional considerations are important:

- Where the breach involves, or may involve, the safety or wellbeing of a young adult at risk, the Data Manager will also follow the organisation's Safeguarding Policy and notify the local authority's safeguarding team. This ensures that safeguarding and data protection responsibilities are met together.

- Lessons learned from any breach will be shared with staff and, where relevant, with the young adults in an accessible way. This supports a culture of openness, accountability, and continuous improvement in line with CQC's well-led and governance standards.