GDPR DATA BREACH POLICY

The Central Team and DPO will review this policy on 2 yearly cycle

Policy Version:	V3
Colleagues affected by this Policy:	All stakeholders
Person responsible for the Policy:	Chief Operating Officer
Approved by/ date:	CEO/ Sept 2021
Next review:	Sept 2023
*Reviewed/ *Next review: (*delete)	
*Reviewed/ *Next review: (*delete)	
*Reviewed/ *Next review: (*delete)	
*Reviewed/ *Next review: (*delete)	
*Reviewed/ *Next review: (*delete)	

Policy Statement
The Sea View Trust holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or stolen or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all staff including governing bodies, referred herein as 'staff'.

Purpose
This breach procedure sets out the course of action to be followed by all staff at The Sea View Trust if a data protection breach takes place. *All data breaches must be reported immediately* to the Executive Leader.

Examples of how a data breach can occur:

- Lost or theft of pupil, staff or governing body data and/or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Hacking
- Offences where information is obtained by deception

"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, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed"

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned." (Statement obtained from ICO).

Immediate Containment/Recovery
The Executive Leader must ascertain whether the breach is still occurring. If so, steps must be taken to minimise the breach:

- Alert IT technician
- Shut down a system
- Attempt to recover lost equipment
- Notify all staff where appropriate

- Change passwords/entry codes
- Written correspondence sent to the wrong recovered
- Emails sent to the wrong recipient recalled or deleted if read

Data Incident Notification Form

Every breach must be fully documented even if it is not necessary to notify the ICO or the data subject. **A Data Incident Notification Form must be completed** (appendix 1) and submitted to the Data Protection Officer (DPO). The DPO'S contact details are as follows:

Data Protection Officer, Forbes Solicitors

dataprotectionofficer@forbessolicitors.co.uk
0333 207 4238

Investigation

The Executive Leader with the assistance of the DPO will lead the investigation to ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The following should be considered:

- The type of data
- It's sensitivity
- What protections are in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people are affected (pupils, staff, parents, governors, suppliers, external agencies)
- If the breach was a result of human error or a systemic issue further investigation or training should be considered to prevent a recurrence
- An action plan should be written following the investigation to identify ongoing issues and what systems need to be in place/changed to prevent future occurrences
- If the breach warrants a disciplinary investigation, the Executive Leader must contact HR for advice and guidance

The DPO will advise:

- whether any further actions need to be taken to contain or recover the data breach
- whether the ICO must be notified (must be within 72 hours of becoming aware of the breach)
- whether the affected data subjects need to be notified

- whether the police (where illegal activity is suspected) or any other services need to be informed

Notification
The Executive Leader should, after seeking the DPO's advice, decide whether the Trust is to proceed in notifying the recommended parties. If the Executive Leader wishes to notify the ICO based on the DPO's advice, the DPO will report the data breach through the appropriate channels.

When reporting a breach to the ICO, the UK GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Implementation
Staff will be made aware of data protection and its requirements during their induction. This policy should be read in conjunction with the Data Protection policy.

Policy review
This policy is reviewed every two years by the Data Protection Officer and the Executive Leader.

The next scheduled review date for this policy is September 2023.

Appendix 1

Data Incident Notification Form

Use this Form to report a potential data breach to the School's Data Protection Officer (DPO). A form should be submitted immediately when you become aware of a potential data breach.

SECTION 1

1. Is the form being submitted on the day the incident occurred? *

2. Name of Employee *

3. School Name*

4. What date and time was the incident discovered? * *We need to understand this because the ICO requires notification within 72 hours of discovery*

5. What date and time did the Incident Occurred *

6. Police and Crime log number (if applicable)

7. Description of the Incident *

8. Has any personal data been placed at risk? *
☐ Data revealing racial or ethnic origin
☐ Political Opinions
☐ Religious or philosophical beliefs
☐ Trade union membership
☐ Sex life data
☐ Sexual orientation data
☐ Gender reassigment data

- [ ] Health data
- [ ] Basic personal identifiers, eg. name, contact details
- [ ] Identification data, eg. usernames or passwords
- [ ] Economic and financial data, eg. credit card numbers, bank details
- [ ] Official documents, eg. Driving licences
- [ ] Location data
- [ ] Genetic or biometric data
- [ ] Criminal convictions, offences
- [ ] Not yet known
- [ ] Other

9. Approximately how many pupils/parents/employees (data subjects) have been affected? *

10. Who has been affected? *

11. Have you informed the data subjects that this incident occurred? If so, when did you do this and how? What was the outcome? *

12. Has there been any media coverage of the incident? If so please provide details

13. Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so please provide details

14. Have you taken any action to prevent similar incidents in the future?

If you have any queries regarding the completion of this form, please contact dataprotectionofficer@forbessolicitors.co.uk

SECTION 2 to be inserted and completed by the Data Protection Officer.