Clyst Vale Community College Data Breach Policy

Contents

Next review date: Sept 2018

Last reviewed: May 2018

1. AIM

The aim of this policy is to standardise Clyst Vale's response to any data breach and to ensure that we log and manage data breaches in accordance with the GDPR law and best practices

This will ensure that:

- Incidents will be reported quickly and can be thoroughly investigated
- Incidents will be dealt with in a timely manner and normal working operations can be restored as quickly as possible
- Any breach Incidents are recorded and also documented fully
- Quick understanding of the impact of an incident, and swift action taken to prevent further issues
- The data subjects and ICO are informed if the severity justifies reporting
- Incidents will be reviewed and processes and procedures improved to prevent repeat

2. DEFINITION

Article 4 (12) of the GDPR states that a data breach is:

"a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

Clyst Vale is required under the GDPR to act when a breach occurs. This procedure sets out how Clyst Vale Community College will respond to a suspected data breach.

This will ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the breach is fully investigated and reported, and any necessary action is swiftly taken to resolve the incident.

A personal data security breach can come in many forms, the most common being:

- Theft, or loss of paper or other hard copies
- Personal data sent via a postal service, e-mailed or faxed to an incorrect recipient
- Theft or loss on devices on which personal data is stored
- Inappropriate sharing or dissemination. Staff accessing information to which they are not entitled
- Virus, hacking, malware and data corruption
- Information is obtained by deception or fraudulent actions
- Equipment failure, flood or fire

- Visitors accessing data that are not relevant to them
- Improper destruction and disposal of data

Where staff are uncertain whether a specific incident constitutes to being a breach of security, either report it to the Data Protection Officer (DPO) or the Senior Information Risk Owner (SIRO). If the issues are regarding a security breach of the network, the IT department should be informed immediately.

3 . SCOPE

This policy applies to all at Clyst Vale, regardless of the data format and is applicable to all staff, visitors, contractors, partner organisations and data processors acting on behalf of Clyst Vale

4. RESPONSIBILITIES

Information users:

The GDPR applies to both Data Controllers (Clyst Vale) and to Data Handlers and Data Processors. All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Managers:

Heads of Subjects and Departments are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required. The DPO will be responsible for overseeing the management of the breach. Suitable further delegation may be appropriate in some circumstances.

5. REPORTING A DATA BREACH

Suspected data security breaches should be reported promptly to the DPO as the primary point of contact at email: i-west@bathnes.gov.uk

The report must contain full and accurate details of the incident including who is reporting the incident, and specify the type of data involved. The report form should be completed as part of the reporting process. See FORM A

Once a breach has been reported, an initial assessment will be done to establish the severity of the breach.

All data security breaches will be logged by the DPO ensuring appropriate oversight into the types and frequency of confirmed incidents for management and reporting purposes. External Article 33 of the GDPR requires Clyst Vale or the DPO (as the Data Controller) to notify the ICO only when the breach "*is likely to result in a risk to the freedoms and rights of natural persons*". A breach of this severity must also be communicated to the data subject (with certain exceptions). Notification must be made "without undue delay" and within 72 hours of becoming aware of it. If Clyst Vale fails to do this, we must explain the reason for the delay. Article 33(5) requires that Clyst Vale must record and

maintain documentation on data breaches. This should include the nature of the breach and the remedial action taken.

When reporting to the ICO, details of the breach must contain information as to the nature of the breach, categories of data,, number of data records, number of people affected, name and contact details of our DPO, and the likely consequences of the breach as well as any action already taken.

6. DATA BREACH PLAN

Clyst Vale's response to any reported data security breach will involve the following four elements:

1. Containment and Recovery
2. Assessment of Risks
3. Consideration of Further Notification
4. Evaluation and Response

Each of the above elements will need to be conducted in accordance with the checklist. An activity log recording the timeline of the incident management should also be completed.

Note: This reflects current guidance from the ICO, which is likely to change

7. DISCIPLINE

Staff, contractors, visitors or partner organisations who act in breach of our policy may be subject to disciplinary procedures or other appropriate sanctions.

8. REVIEW

This Policy document will be subject to annual review by SLT, Governors and DPO

9. SOURCES

- The GDPR https://gdpr-info.eu
- ICO GUIDANCE ON DATA BREACHES https://ico.org.uk/media/fororganisations/documents/1562/guidance_on_data_security_breach_management.pdf

FORM A - Reporting a data breach template

	Reported by:	**Name:** **Job Title:** **Date:**
A	Summary of event and circumstances	Eg. Who, what, when, who
B	Type and amount of personal data	Eg. Title of document(s) / information included / name / contact details / financial / sensitive / special category data.
C	Action taken by recipient	
D	Action taken to retrieve data and respond to breach	
E	Procedure/policy in place to minimise risk	Eg. Communication, secure storage, sharing, exchange.
F	Breach of policy/procedure by officer/member	Eg. Has there been a breach of policy and has appropriate management action been taken?
G	Details of notification to data subject. Complaint received?	Eg. Has the data subject been notified? If not, explain why. What advice has been offered?
H	Details of GDPR training provided.	Eg. Date of most recent training by staff involved
I	Risk assessment and changes need to prevent further data loss	
J	Conclusions and learning points	
