Davenant Foundation School

Security Incident Policy

This policy has been reviewed and to the best of our knowledge, we do not feel that it impacts on any group or individual's equality rights within our school community

Last Reviewed: **March 2020**

Next Review: March 2021

Policy Name:	**Security Incidents Policy**	**Committee Responsible**	**Standing / Personnel**
Status	**Mandatory**	**Committee Person i/c**	**DHL / AT**
Produced by	**G Casson**	**First Agreed**	**March 2018**
Date Produced	**February 2018**	**Last Review Date**	**March 2020**
References	**GDPR – May 2018**	**Next Review Date**	**March 2021**

Security Incidents Policy

A security incident is a confirmed breach, potential breach or 'near-miss' breach of one of Davenant Foundation School's Information Policies

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST***: If you discover a security incident, you must immediately **report** it
2. ***MUST***: When reporting the incident, you must **provide** as much information as possible
3. ***MUST***: The *Investigating Officer/ Line Manager* must **complete** investigations as directed by the Head Teacher and complete an outcome report (see Procedures for Reporting or Handling a Security Incident)
4. ***MUST***: The Head teacher must support investigations as directed by the Investigating Officer and provide an **outcome report**
5. ***MUST***: The Head Teacher / Compliance Officer must oversee and support each investigation, maintaining a full **record** from reporting to closure
6. ***MUST***: The Head Teacher /Compliance Officer / DPO must support the investigation of **major and critical** incidents
7. ***MUST***: Comply with the timescales and escalation process outlined in our Procedures for Reporting or Handling a Security Incident.
8. ***MUST***: In the event that a security incident is detected out of hours, the Head Teacher and/or SLG Duty Supervisor **must** be alerted immediately.

Why must I do it?

1. Capturing security incidents allows us to respond effectively when something has gone wrong. Capturing all types of security incidents allows us to understand where our weaknesses are, how well our policies are working and what we should change about our policies to make them more effective
2. To help us quickly assess the severity of the incident and to speed up the investigation
3. Carry out an effective process appropriate to the severity of the incident
4. Carry out an effective process appropriate to the severity of the incident
5. Ensure the process is followed to completion
6. Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact incidents
7. Ensure that all incidents are handled in a timely manner.

8. To enable the Head Teacher and/or SLG Duty Supervisor to quickly assess the severity of the incident, and decide if it needs to be reported to the DPO and/or the regulator.

How must I do it?

1. Staff must report all security incidents in person or by email to The Head Teacher / Compliance Officer. If you would like to stay anonymous you may do so, by reporting the incident in writing to the Head Teacher and/or Chair of Governors. No action will be taken against any member of staff who reports a security incident about another member of staff in good faith. Identification of a reporting party who requests anonymity shall be protected as far as is feasible.
2. Include full details of the incident such as dates, names and any remedial action that has been taken.
3. Where appropriate, undertake the following:
    a. Identify expected outcomes, stakeholders and any policies breached.
    b. Speak to staff involved.
    c. Record evidence and keep an audit trail of events and evidence supporting decisions taken
    d. Get expert help
    e. Escalate
    f. Inform data subjects (service users, staff) where appropriate
    g. Identify and manage risks of the incident
    h. Commence disciplinary action, or record why not
    i. Develop and implement a communications plan where appropriate
    j. Put in place controls to prevent recurrence
    k. Complete the Incident Outcome Report
4. Where appropriate, undertake the following:
    a. Work with the SIRO to investigate major security incidents.
    b. Assess the outcome to ensure the appropriate action has been taken.
    c. Provide knowledge and advice, and carry out any recommended actions for major or critical incidents, where required.
5. Undertake the following:
    a. Classify the Security Incident
    b. Verify the details and oversee the investigation
    c. Work with The Head Teacher / Compliance Manager to investigate major security incidents.
    d. Advise, support and intervene as appropriate

    e. Review Incident Outcome Reports and close
6. For major and critical incidents:
    a. Undertake the investigation (critical only)
    b. Work with The Head Teacher / Compliance Manager / DPO (major only)
    c. Assess if it is necessary for the security incident to be reported to the ICO.
    d. Complete an outcome report and recommend remedial actions.
7. Follow the process outlined in the Davenant Foundation School Procedures for Reporting or Handling a Security Incident
8. Out of hours, security incidents must be reported to the Head Teacher, and/or Duty Supervisor by telephone and/or email. (use personal mobile for Head Teacher, if unable to contact via email.)

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting The Head Teacher of Davenant Foundation school.

If you believe the policy does not meet your business needs, you may raise this with your Information Champion who, if they agree with your suggestion, may propose a policy change.

Document Control

Version:	2
Date approved	- March 2020
Approved by:	Standing Committee – Davenant Foundation School
Next review:	March 2021 – Reviewed Annually

References

- Data Protection Act 1998 (to May 25th 2018)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.