SHARD Business Services

DATA BREACHES

A Practical Guide for Schools and Academy Trusts

Data breaches can happen quickly. Schools and trusts need a calm, evidenced response that contains the incident, assesses risk and reports where required.

Every breach must be assessed, recorded and handled proportionately. Fast action reduces harm and supports accountability.

SIX FOUNDATION PRINCIPLES

1 RECOGNISE THE BREACH

Know what counts as a breach, including loss, theft or unauthorised disclosure.

Key Message: Act early.

2 CONTAIN THE INCIDENT

Secure systems, recover information and prevent further disclosure or harm.

Key Message: Limit impact.

3 ASSESS THE RISK

Consider the data, people affected and likely impact on rights and freedoms.

Key Message: Evidence judgement.

4 REPORT WHERE NEEDED

Notify the ICO within 72 hours where the risk threshold is met.

Key Message: Do not delay.

5 INFORM INDIVIDUALS

Tell affected people promptly where there is a high risk to them.

Key Message: Be clear.

6 REVIEW & IMPROVE

Learn from incidents and strengthen policies, training and controls.

Key Message: Improve practice.

FIVE KEY ACTIONS

RECOGNISE
Log the incident.

RESPOND
Contain and secure data.

ASSESS
Evaluate risk.

REPORT
Notify ICO if required.

IMPROVE
Strengthen controls.

DATA BREACH EXAMPLES

01 Accidentally sending an email containing personal data to the wrong recipient.

02 Intentionally or accidentally amending personal data without consent or permission.

03 Safeguarding information being shared with unauthorised people.

04 Accessing the system using somebody else's username and password.

05 Losing a USB stick, documents, or a mobile device which contained personal information.

REMEMBER

It is essential that you know how to recognise data breaches, as there is an obligation to investigate data breaches and protect the personal data we hold.

PRACTICAL GUIDANCE

Use this page to respond to suspected data breaches, evidence decisions and strengthen future controls.

GOOD PRACTICE

- ✓ Lock your computer screen whenever you leave your device and set screens to auto lock when periods of inactivity are detected.
- ✓ If you're unsure about who is contacting you, check with somebody
- ✓ Backing up your systems and then testing you can retrieve your data.
- ✓ Implement a clear desk policy.

Embed what good looks like.

- ✓ Avoid using portable media devices, such as USB drives unless fully encrypted.
- ✓ Keep work and personal emails separate – don't be tempted to mix the two.
- ✓ Do not download attachments from senders that you do not know.
- ✓ Anonymise personal identifiable data wherever possible.

THE 5 KEY ACTIONS

1 RECOGNISE
Spot a potential breach and log it immediately.

2 RESPOND
Contain the incident and protect records or systems.

3 ASSESS
Assess risk to rights and freedoms.

4 REPORT
Report to the ICO within 72 hours where required.

5 IMPROVE
Review causes, train staff and strengthen controls.

SELF-ASSESSMENT CHECKLIST

	Yes	No	N/A
We have a clear breach response process.	☐	☐	☐
Staff know who to contact immediately.	☐	☐	☐
We maintain a breach log and decision record.	☐	☐	☐
We assess ICO reporting requirements promptly.	☐	☐	☐
We review incidents and improve controls.	☐	☐	☐
Lessons learned and actions are recorded.	☐	☐	☐

USEFUL CONTACTS & RESOURCES

ICO: Personal data breaches
Reporting and risk assessment guidance

DfE: Data protection in schools
Managing breaches of data

UK GDPR Articles 33-34
Notification and communication duties

NCSC Cyber Security Guidance
Incident response support

SBS Resources
Templates and support available on request