Devonshire Primary Academy Data Breach Policy

Policy Statement
Devonshire Primary Academy 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 Devonshire Primary Academy if a data protection breach takes place. *All data breaches must be reported immediately* to the Headteacher.

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-GDPR – what is a personal data breach?)

Immediate Containment/Recovery
The Headteacher must ascertain whether the breach is still occurring. A Data Breach Record must be completed (appendix 1) and 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

- Notify the Data Protection Officer (DPO)
- Consideration whether the police (where illegal activity is suspected) or any other services need to be informed
- Is legal advice needed?
- Does the ICO need to be notified? (Must be within 72 hours of becoming aware of the breach.)

Notification

Some people/agencies may need to be notified as part of the initial containment. The Headteacher should, after seeking expert or legal advice, decide whether anyone should be notified of the breach. Every breach must be fully documented even if it not necessary to notify the ICO or the data subject. When reporting a breach, the 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

Investigation

The DPO will fully investigate the breach. The Headteacher should 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
- Its 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 investigator must contact HR for advice and guidance

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 and the Privacy Notice.

Appendix 1

Data Breach Record

Date Reported	Time Reported
Name of person reporting the breach	
Initial person responsible for dealing with breach	
Which data subjects are involved (staff, pupils etc.) Include approximate numbers	
Data type involved (personal, sensitive financial etc.) A personal data breach is an incident that has affected the confidentiality, integrity or availability of personal data	
Is the breach considered to be High Risk ☐ Low Risk ☐ (Is the breach a high risk to the rights and freedoms of the individual(s))	
Is the data sensitive Yes ☐ No ☐	
How did the breach occur: ▪ Access by an unauthorised third party ▪ Deliberate or accidental action (or inaction) by a controller or processor ▪ Sending personal data to an incorrect recipient ▪ Computing device containing personal data being lost or stolen ▪ Alteration of personal data without permission ▪ Unlawful destruction of personal data without permission ▪ Loss of availability of personal data (accidental or otherwise) ▪ Other	

Who has gained access to the data	
What has happened to the data?	
What is the likely consequence of the data breach?	
What immediate actions have taken place (e.g. password changes/ IT tech notified)	
Have staff been notified (if appropriate)	
Has data subject(s) been notified (if appropriate)	
Contact made with DPO (state time, date and method of notification	
Contact made with ICO (this must be done within 72 hours of becoming aware of the breach) Tel 0303 123 1113 Mon-Fri 9-5pm (Wed until 1pm) *If ICO not contacted document why not here*	
What preventative action will take place to prevent a further recurrence (include training)	

Signed _____

Position _____

Date completed _____