Castleton CE Primary School Data Breach Procedure

Types of breach

Data protection breaches could be caused by a number of factors. A number of examples are shown:

- Loss 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.
- Poor data destruction procedures.
- Human error.
- Cyber-attack.
- Hacking

Managing a data breach

In the event that the school identifies or is notified of a personal data breach, the following steps will be followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, the School Business Officer and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this will begin as soon as is practicable.

2. The Head Teacher or DPO (or nominated representative) will ascertain whether the breach is still occurring. If so, steps will be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Head Teacher or DPO (or nominated representative) will inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher or DPO (or nominated representative) will also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support will be obtained.

5. The Head Teacher or DPO (or nominated representative) will quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempting to recover lost equipment.

- Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration will be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher or DPO (or nominated representative).

- Contacting the County Council's Communications Division if part of the crisis service, so that they can be prepared to handle any press enquiries. The Council's Senior Communications Officer can be contacted by telephone: 01629 538234

- The use of back-ups to restore lost/damaged/stolen data.

- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or IT system passwords, then these will be changed immediately and the relevant agencies and members of staff informed.

Notifying other people or agencies

Some people or agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher or DPO (or nominated representative) will, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident will be considered on a case by case basis.

When notifying individuals, we will give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. We will also give them the opportunity to make a formal complaint if they wish. The notification will include a description of how and when the breach occurred, what data was involved and include details of what the school has have already done to mitigate the risks posed by the breach.

Review and evaluation

Once the initial aftermath of the breach is over, the Head Teacher or DPO (or nominated representative) will fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan will be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation will liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher or DPO will ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This will be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

Data breach checklist:

Action	Taken? Give dates, initials and links to docs where appropriate
Date and time of discovery	
Date and time of occurrence	
Immediate steps taken to contain the breach, eg changing passwords, shutting computers down, halting network traffic, restore data from backups	
Acknowledge breach by thanking informant for information – log it here	
Inform DPO	
DPO inform HT	
Letter acknowledging breach sent out	
Type of breach	☐ Loss / theft / unauthorised access of pupil, parent, staff or governing body data ☐ Loss / theft / unauthorised access equipment on which data is stored ☐ Inappropriate access controls allowing unauthorised use ☐ Equipment failure ☐ Poor data destruction procedures ☐ Human error ☐ Cyber-attack ☐ Hacking
Investigation	1. What happened 2. When it happened 3. How it happened 4. How many people could be affected? 5. What sort of data has been breached? 6. What did you have in place that could have stopped it? 7. What have you done to help the people this affects? 8. What have you learned? 9. How can you stop similar breaches in the future?
Necessary to inform ICO? 0303 1231113	
Date and time reported to ICO	
Data subjects informed?	
Police informed	
Steps taken to avoid reoccurrence	
Concluding letter	
SLT / Governors de brief	
Report completed by	