COOMBE HILL INFANTS' SCHOOL

For more information please contact the school's Data Protection Officer (DPO) Jackie Patel on 020 8942 9481 or jpatel164.314@lgflmail.org

DATA SECURITY BREACH FLOWCHART

Containment and recovery

Investigate the breach to ascertain the severity and determine if any personal data is involved/compromised. Identify the cause of the breach to help ensure that it can be contained as much as possible. Implement further action to recover lost or damaged data. Contain further data loss – e.g. take systems offline, back up and encrypt all existing data. Where appropriate, notify the police of the security breach.

Assessment of risks

Assess the data breach to determine: how much data is involved, the personal nature and sensitivity of it, what has happened to it, whether it is protected/encrypted, whether back-ups are in place, and whose data is compromised, and how. Mitigate potential harm to individuals or the school community – this could include physical safety, emotional wellbeing, reputation, finances, identity or private affairs, and any threats to public reputation or general operations.

Consideration of further notification

Assess if there are any legal, contractual or regulatory requirements, or if parties could act on the information to mitigate risks. Communicate to any relevant parties: how and when the breach occurred, what data it involved, containment measures in place, specific and clear advice on protecting themselves, and channels they can communicate concerns via. Look to notify any third parties – police, insurers, professional bodies, banks etc. – who can assist in helping mitigating the impact on individuals. Under the GDPR the ICO is notified within 72 hours of a breach where it results in a risk to the rights and freedoms of individuals. If personal data is compromised, directly notify affected individuals about the extent and nature of the breach.

Evaluation and response

Establish the root of the breach and where any current of future risks lie. Identify any weak points in existing security measures and procedures, and recommend appropriate measures for the future. Identify any weak points in levels of security awareness and training among staff, and recommend new strategies and processes. Report on assessment findings and, with the approval of school leadership, implement the recommendations of the report after analysis and discussion.

Review of process

Ensure there has been compliance with relevant regulations and legislation throughout the process. Review the efficiency and effectiveness of the breach management plan and those in charge of it. Review the process at regular intervals to keep it up-to-date.