Fountaindale
Believe, Achieve, Succeed

Review date: July 2019

An outline of the Organisational and Technical Security Measures deemed appropriate by the Data Controller for the nature of the personal data processed by the Controller and any Data Processors acting on its behalf

Fountaindale School
Nottingham Road
Mansfield
Nottinghamshire NG18 5BA

Nottinghamshire County Council
in partnership with
Essex County Council

Description of Security Measures employed to safeguard the processing of Personal Data

1. Policies & Documented Procedures

1.1 Fountaindale School is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

1.2 Our policies are informed by Nottinghamshire County Council and conform to statutory requirements. They inform and reflect Fountaindale School's practice. All policies have documented review dates and ownership is assigned to the Governing Body. Reviews are held ahead of the expiry date or sooner where there is an identified issue or change. All policies follow a governance route for approval. Key policies are published to the Fountaindale School's website for transparency. Copies of policies are available on request.

1.3 The purpose of this policy is to:

- protect against potential breaches of confidentiality;
- ensure all our information assets and IT facilities are protected against damage, loss or misuse;
- support our data protection systems by ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data;
- increase awareness and understanding within Fountaindale School of the requirements of information security and the responsibility of all staff to protect the confidentiality and integrity of the information that they themselves and other staff members handle.

2. Roles.

2.1 Fountaindale School has a named Data Protection Officer, who is Anita Buffrey. This Officer executes the role by reporting the outcome of the statutory process to The Principal, Stuart Cameron, who acts as the Fountaindale School's Senior Information Risk Owner.
The DPO provides reports to the Governing Body, who oversee the implementation of this policy. The governor for G.D.P.R is Elaine Jeffery.

3. Training

3.1 Fountaindale School regularly reviews our employee roles to ensure that training and awareness messages are appropriate to the nature and sensitivity of the data processing undertaken. Induction processes ensure new employees receive appropriate training before accessing personal data, and all other employees receive refresher training annually. All training received is documented for evidence purposes.

4. Risk Management & Privacy by Design

The organisation identifies information compliance risks on its risk register. Risks are assigned clear ownership, rated against a consistent schema, appropriate mitigations are identified and are annually reviewed.

4.1 All Data Processors handling personal data on behalf of Fountaindale School have given assurances about the compliance of their processes; either through procurement assurances/ evidence, contractual agreement controls, risk assessments or supplementary statements.

4.2 Third parties should only be used to process Fountaindale School information in circumstances where written agreements (GDPR statement of use) are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings.

4.3 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the Principal or Vice Principal for more information and inform the Office Manager of any arrangements with third parties.

4.4 The Office Manager is responsible for up-dating and maintaining a record of external / third parties and storing relevant evidence of compliance.

5. Physical Security

5.1 All employees who have access to Fountaindale School premises, where personal data is processed, are provided with Login Cards which validate their entitlement to access.

5.2 Fountaindale School operates a secure process which ensures only those individuals who have an entitlement to access the premises are able to. Access to physical storage holding sensitive personal data is further restricted either through lockable equipment with key or code control procedures or through auditable access to specific rooms/ areas of buildings.

5.3 Access to offices and information - Office doors must be kept secure at all times and visitors must not be given keys or login cards to access areas identified, that hold/store data.

5.4 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by or be fitted with privacy screens.

5.5 Visitors will be required to sign in at reception, and never be left alone in areas where they could have access to confidential information.

5.6 Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room, which contains personal data or information, then steps should be taken to ensure that no confidential information is visible.

5.7 At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away and office doors locked to limit access.

6. Security Incident Management

6.1 Fountaindale School maintains a security incident process which, with the support of appropriate training, defines what constitutes a breach of these security measures to facilitate reporting of incidents. The process covers investigation of incidents, risk rating and decisions over whether to notify an incident to the Information Commissioner's Office (ICO) within the statutory guidelines and timescale. Incidents are reported to senior leaders, and actions are taken and lessons learned implemented.

6.2 All staff have an obligation to report actual or potential data protection compliance issues, failures to the DPO This allows Fountaindale School to investigate the issue, failure and take remedial steps if necessary; make any applicable notifications.

7. Data Handling & Protection

7.1 Use of Hosting Services - some personal data is processed externally to Fountaindale School's managed environment by third parties in data centres under agreed terms and conditions, which evidence appropriate security measures.

7.2 Firewalls - access to the Fountaindale School's managed environment is protected by maintained firewalls. Business needs to provide access through the firewall go through a strictly documented change control process which include risk assessment and approval.

7.3 Administrator Rights - enhanced privileges associated with administrator accounts are strictly managed by the Principal and Vice Principal. Administrator activities are logged and auditable to ensure activity can be effectively monitored.

7.4 Access Controls - access permissions to personal data held on IT systems is managed through role based permissions. The Principal and Vice Principal inform the IT technician of additions, amendments and discontinuation of individual accounts within permission groups. Managers are periodically required to confirm that current permissions for which they are the authoriser and employees associated with these permissions are accurate.

7.5 Password Management - Fountaindale School sets a mandatory password complexity combination of minimum length and characters.

Staff should:

- Use password protection and encryption where available on Fountaindale School systems to maintain confidentiality.
- Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis.
- Passwords should not be written down or given to others.
- Computers and other electronic devices should be locked when not in use to minimise the risk of accidental loss or disclosure.
- Confidential information must not be copied onto removable hard drive, CD, DVD, memory stick or any portable storage device without the express permission of the Principal or Vice Principal, the device and information must be encrypted.

- Data copied onto any storage devices should be deleted as soon as possible and stored on Fountaindale School's secure computer network in order for it to be backed up.
- All electronic data must be securely backed up at the end of each working day.

7.6 Anti-Malware & Patching - Fountaindale School has a documented change control process which facilitates the prompt implementation of any security updates provided by the suppliers of active software products.

7.7 Disaster Recovery & Business Continuity - As part of Fountaindale School's business continuity plan, there is provision to ensure effective processes are in place to both safeguard personal data during a service outage incident and to re-establish secure access to the data to support data subject rights in ongoing service provision.

8 Data in Transit

8.1 Secure email- sensitive data will be sent using a system of encrypting and password protecting sensitive data in email attachments.

8.2 Fountaindale School has access to third party websites which allow for secure upload of personal data. The organisation uses these facilities to fulfil statutory obligations to report personal data to other public authorities.

8.3 Staff should ensure they do not introduce viruses or malicious code on to the Fountaindale School systems.

8.4 Hard-Copy Data -The removal of personal data in hard-copy form is controlled by Fountaindale School policy, which requires employees to take steps to conceal the data and appropriately secure the data during transport and use of site.

8.5 These security measures are reviewed annually and approved as accurate and appropriate by Fountaindale School's governance process.

8.6 Staff should not take confidential or other information home without the permission of the Principal / Vice Principal and only do so where satisfied appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information.

8.7 In the circumstances in which staff are permitted to take Fountaindale School information home, staff must ensure that:

- Confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors;
- All confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.
- Staff should not store confidential information on home computers or electronic devices.

8.8 There are restrictions on international transfers of personal data. Staff must not transfer personal data internationally at all without first consulting the Principal.

9 Communication of Information

9.1 Staff should be mindful about maintaining confidentiality when speaking in public places. Especially, but not limited to, using names of pupils, staff, parents, governors or associates of the school.

9.2 Confidential information should be marked 'confidential' (electronic and hard copies) and circulated on a need to know basis in the course of their work/duties for Fountaindale School.

9.3 Confidential information must not be removed from Fountaindale School offices or files without permission from the Principal or Vice Principal, except where that removal is temporary and necessary.

9.4 In the limited circumstances when confidential information is permitted to be removed from Fountaindale School's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained.

9.5 Staff must ensure that confidential information is:

- Not transported in see-through bags or folders
- Be in secured bags or cases;
- Not be read in public places, in view of the public (eg waiting rooms, cafes, trains);
- Not be left unattended or in any place where it is at risk (eg in conference rooms, car boots, cafes).

9.6 Mis-placed or lost information must be reported immediately to the Principal, Vice Principal and DPO.

9.7 The Principal / Vice Principal must take appropriate steps to recover misplaced or lost information immediately.

9.8 Postal and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

9.9 All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by hand, tracked or recorded delivery.

9.10 Sensitive or particularly confidential information **should not** be sent by fax unless it is confirmed that it will not be inappropriately intercepted at the recipients address.

10. Reporting breaches & Consequences

10.1 All staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows Fountaindale School to: investigate the failure and take remedial steps if necessary; make any applicable notifications.

10.2 Fountaindale School takes compliance with this policy very seriously. Failure to comply puts Fountaindale School, its staff and pupils at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

10.3 Staff with any questions or concerns about anything in this policy should not hesitate to contact the Principal or Vice Principal.

11. Review and training

11.1 The Principal is responsible for this policy.

11.2 Fountaindale School regularly monitors the effectiveness of this policy to ensure it is working in practice. This policy will be up-date as required and reviewed annually.

11.3 Fountaindale School will provide information and/or training on any changes made.

11.4 All staff will receive appropriate training on this policy, including training on any updates

11.5 All staff must sign a central record to confirm they have received, read and accept the terms and conditions of this policy. This record will be stored in the school office.