Madresfield C.E. Primary School

Data Security / Data Protection Policy - January 2017

1. Introduction

This document defines the basic security requirements that must be met when processing, storing and handling data to ensure that data is held securely and only accessed by those authorised to do so.

It is the responsibility of all parties accessing schools' IT systems to comply with the requirements of these guidelines.

2. Data Security definition:

Data security legislation means that all those who hold personal data, whether on paper or electronically, must keep that data secure. Clearly, this also applies to schools. Personal data is defined as any combination of data items that identify an individual and provide specific information about them, their families or circumstances. This includes names, contact details, gender, date of birth, as well as other sensitive information such as academic achievements, other skills and abilities, and progress in school. It also includes behaviour and attendance records.

The biggest risk to data security is posed by how users manage the security of that data. This means all staff members in school.

3. Passwords

All staff must ensure that sensitive information is physically secured or password protected.
In order to minimise the risk involved in accessing the IT systems users are required to adhere to the following:

- Always follow your schools password procedure
- Always log out, or "lock" the screen when leaving your computer unattended
- 'Strong' passwords should be used – don't use simple or obvious passwords
- Never share passwords with others, never tell your password to anyone
- Never write passwords down and leave them near the computer
- Don't use work passwords for personal online accounts
- Don't save passwords in web browsers
- Never use your user name as a password
- Never email your password or use it in an instant message

It is your personal responsibility to ensure your device is kept secure, in accordance with the following guidelines.

4. Data Protection

- Staff must comply with the Data Protection Act and the school's Acceptable Use Policy at all times
- Sensitive data must never be copied to unauthorised locations/devices (e.g. USB Memory sticks, Home PCs, etc.) – remember that databases may contain sensitive data
- Data must be accurate, relevant and current
- Master documents need to be secure and backed up – data should never be solely stored on an external device (e.g. a USB Memory stick)
- When deleting sensitive data, ensure you also empty the Recycle Bin
- Mobile devices (such as laptops, XDAs or external hard disk drives) are subject to the same security considerations as any other computer

5. Equipment Security

- IT Equipment holding sensitive data must be encrypted
- IT Equipment issued to staff remains the responsibility of that individual at all times - they must never be "loaned" to another individual (including family members)
- Laptops and all other mobile devices (e.g. USB Memory sticks) must be kept secure at all times
- Never leave your laptop or computer unattended in a vehicle as this would invalidate any insurance claim - this includes leaving equipment in the boot of the vehicle
- All staff laptops must connect to the school's network at least once each ½ term to allow for software and anti-virus updates

6. Other good practice

- Always turn off your computer using the Shut Down option – never use Standby, Sleep or Hibernate and never just close the lid (laptops)
- Beware of people watching as you enter passwords or view sensitive information
- Always store equipment securely (e.g. use the hotel-safe when travelling, etc)
- Always keep remote access tokens/dual-factor login fob separately from your laptop
- Don't leave equipment unattended in an unsecure location
- Don't use public wireless hotspots

School laptops and equipment are for the sole use of authorised school users.

For further information please refer to the IBS Schools System and Data Security document which can be found on the IBS Schools website at http://www.capita-sims.co.uk/ibs-schools

Records and Documents

Sensitive documents are to be held in a locked cabinet in the school, this includes information linked to child protection and safeguarding and staff and children's files. There must be restricted access to these documents.

All SEND files are to be kept in a locked cupboard. There must be restricted access to these documents.

Retention, destruction and archive policy

Staff must retain the documents in accordance with current guidelines and check the current status before they destroy or pass on information.

Sensitive documents are to be shredded when they are no longer needed.

Copies of child protection files are to be taken as necessary before passing them on to another school. They are to be signed for and a copy kept.

Archived information is to be stored in a secure cupboard.

Ratified by the Governing Body on 10th January 2017

Review Date: January 2019