St. Margaret's Anfield Church of England Primary School

Jesus said, "Love one another as I have loved you" (John 13:34). Therefore, by faith and work, be the change you want to see.

With God, all things are possible.

Data Protection Procedure & Responsibilities

Ms V Whitfield

Date	Action	Review Date
July 18	Version 1 Adopted by FGB	Mar 23
March 23	Version 2 Adopted by FGB	Mar 24

Policy Overview

- to educate staff about the procedures they must adhere to in handling personal data
- to help comply with the duty of the school to protect the security of personal data, by informing staff of necessary measures

What It Covers

- personal data
- data breaches
- responsibilities of data handling
- data breaches reporting

Staff are expected to adhere to this policy and protect personal data from security risks.

Personal Data

Personal Data
Personal data is information that relates to an identified or identifiable individual. It can fall into two categories - the first being basic information such as the examples below:

- First and Surnames
- Date of Birth
- Home Address
- Postcode

The second category is what's officially known as '**Special Category Data'**. This means it much more sensitive information and as such, is much more tightly controlled. Examples include:

- Race
- Ethnic Origin
- Religion

As a school we handle both categories of personal data every day – so it's important to learn the difference between the two.

Data Breach

A personal data breach means a breach of security leading to the accidental or purposeful, loss or access, to personal data (listed above).

A typical scenario that may occur in a school, involving a data breach would be;

- a paper copy of pupil information (e.g. names, addresses, religion) being left on a coach after a school trip

- an unencrypted memory stick/ hard drive is lost outside the school holding pupil information (e.g. end of year reports, class lists)

In every instance a data breach occurs it must be reported to the school.

Responsibilities

Data Handling

At any time, personal data is handled – you become solely responsible for ensuring it is secure.

- personal data is information that relates to an identified or identifiable individual and I'm aware of the two categories it can fall into.
- Staff have a responsibilty to use reasonable measures to protect any and all personal data they handle.
- Staff should at all times follow 'good practice' when handling personal data as set out in the bulletpoints in this policy.
- Staff understand what constitutes a data breach and agree to follow the data breach reporting procedure.

Paper Copies

- Paper copies should always be handled with due care and consideration.
- Any paper copy of personal data should only be kept for as long as it is needed.
- Where a paper copy is no longer needed, it **must** be disposed of using one of the public shredding bins located at the Infant Photocopier, Welfare Office or Staffroom.
- If a paper copy is to be retained for an extended or permenant period of time, then a reasonable attempt **must** be made to store it safely.
  A safe area must have restricted access and locked if possible (examples include a desk draw or class cupboard). If stored in a public area this is required to be locked.
- Duplicate copies are not to be made unless required and approved by SLT.

Electronic Copies

- Never save sensitive electronic copies of data to the shared network drives unless others are required to view them.
- Remember to always save electronic copies of data to your own documents where possible – you should never save to a public area by default.
- Never share electronic copies of data externally unless explicitly required.
- An encrypted storage device is required in every instance to hold electronic copies of data.
- Where an electronic copy is no longer needed it must be deleted, this also includes deleting it from the 'Recycle Bin'.

Data Breach Reporting

Data Breach Reporting

You are required to report any of possible loss of personal data to the SLT.

- This must be reported by the end of the school day or alternatively before 9am of the next day if this is not possible.
- Any loss of equipment that holds personal data such as a memory stick or laptop must also be reported using the same time scale.