Information Protective Marking Scheme

24-25

Reviewed by Governors: March 2025

To be reviewed: March 2026

Introduction

Information sharing between professionals is vital to ensure the wellbeing of Children. Park Brow Primary School aims to fulfil its obligations to the fullest extent and will follow the "7 Golden Rules of Information Sharing" described by the DfE:

1. Remember that GDPR is not a barrier to sharing information
2. Be open and honest with the person or family
3. Seek advice if you are in any doubt
4. Share with consent where appropriate
5. Consider safety and well-being
6. Necessary, proportionate, relevant, accurate timely, and secure
7. Keep a record of your decision and reasons

Information Security

Under principle 6 of the GDPR, the school has a duty to ensure that data is handled securely. To fulfil its obligations under the act and to comply with Cabinet Office guidelines outlined in "Data Handling Procedures in Government" the school will adopt the following to maintain data security:

- Users may not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely for storage in a secure location.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Sensitive or personal data must be securely deleted when it is no longer required.
- Computer passwords should not be disclosed or shared between users
- Files and paperwork that identifies individuals must never be left unattended and must be stored in locked cabinets within a controlled access room that must be locked when not in use
- All staff processing personal information should be appropriately trained

The school will use a protective marking scheme to ensure that all data – electronic or on paper – is labelled according to the protection it requires based on Impact Levels:

Impact level	Colour Code	Memory stick?	Example
IL0–Not Protectively Marked		No	Newsletters, public information
IL1- Unclassified		No	Generic letters to parents containing no personal data
IL2–PROTECT		No	Basic student information such as name and address
IL3–Restricted		No	Sensitive Student information such as ethnicity or FSM status
IL4-Confidential		No	Highly sensitive student data relating to child protection

Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned.

Handling Instructions

- Codewords provide security cover for a particular asset or document. A codeword is a single word expressed in CAPITAL letters. They are most commonly applied to PROTECT, RESTRICTED and CONFIDENTIAL assets. Codewords are centrally allocated; please contact your SSA/SA if you require one for an asset at any tier.
  Codewords go after the classification and the handling instruction. Please see below for an example:
  CLASSIFICATION - HANDLING INSTRUCTIONS - CODEWORD

- Password protected documents provide security for a document or asses. A password should be a mixture of letters, numbers and symbols that do not relate to the child, school or document its self. Passwords should be applied to PROTECTED, RESTRICTED AND CONDFIDENTIAL documents, and should be shared with the receiver of the document via a separate email. The password should never be within the email containing the protected document.

Incident Reporting

GDPR introduces a legal duty to report certain types of personal data breach to the Information Commissioner's Office (ICO); this must be done **within 72 hours** of the school becoming aware of the breach, where feasible, even if all details of the breach are not yet known.

In addition, the school is required to inform the data subjects of the breach without undue delay if it is considered that there is a high risk of the breach adversely affecting their rights and freedoms.

Unauthorised disclosure of personal data is a criminal offence under Section 55 of the Data Protection Act 1998 and will likely lead to disciplinary action

All staff are responsible for ensuring that information is managed according to this policy.