Springside School

Data Handling Procedures Policy

January 2022

Rochdale Schools Network – Springside School
Data Handling Procedures and Guidelines

1. All staff will be issued with ID cards which must be worn when outside school with learners and staff will challenge visitors that are not wearing ID badges or visitor's badges within school.

2. Staff will record all visitors to buildings and wherever feasible ensure that they are accompanied whilst on the premises. Visitors will sign in on the reception desk and be provided with a visitor's Badge which must be worn for the duration of their visit.

3. Staff will implement a clear desk/clear screen policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when areas are unattended. Computers must be turned off at the end of the day.

4. Staff will ensure where personal information is held on paper, it is locked away when not in use or the premises are secured.

5. All unwanted personal information should be securely destroyed: paper records by shredding so that reconstruction is unlikely and electronic media by overwriting or erasure.

6. Wherever possible the use of removable media including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats should be avoided. Where it is unavoidable, encryption **must** be used and the information transferred should be the minimum necessary to achieve the business objective.

7. Access to systems should be restricted to those users that need it. This will be achieved through Active Directory Group Policy and file/folder permissions. Access to raw data will be strictly controlled and only anonymous data should be readily available.

8. Where it is not possible to access information on secure premises and systems, the following hierarchy should apply:

a. Access should be via secure remote access so that information can be viewed or amended without being permanently stored on the remote computer.

b. Next best is secure transfer of information to a remote computer on a secure site on which it will be permanently stored.

c. Decisions on handling/transfer of information should be approved in writing by the relevant information asset owner.

d. User rights to transfer information to removable media should be carefully considered and strictly limited. Where it is necessary to bulk transfer information, it should be done electronically across the secure network.

9. Where information needs to be shared between organisations secure networks must be used. It is never acceptable to transfer bulk personal information via normal e-mail services. The use of the Rochdale Schools Intranet should be utilised to assist in the communication between RMBC, RSN and Secondary School systems.

10. **Review** This document will be reviewed annually.