

Buttsbury Junior School

Data Protection in Practice

Spring Term 2019



This document is based on a template provided by SBM Services (uk) Ltd and is only authorised for use by those schools in contract with SBM Services (uk) Ltd. This template may not be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of SBM Services (uk) Ltd.

Copyright © 2018 All rights reserved

Data Protection in Practice

Physical records

- Do not leave confidential or restricted documents out on desks or display if the room is unoccupied or if it can be accessed by others.
- Lock cupboards, drawers or other storage units that contain confidential documents.
- Minimise, wherever possible, the amount of personal data used in classroom displays

Confidential Discussions

- Do not conduct confidential discussions in front of unauthorised individuals.
- Do not write down opinions, (by email or hard copy), about a person that you would not feel comfortable saying to their face. Record facts not opinions.

Electronic data

- Personal information should be password protected before sending by email and the password conveyed separately.

Passwords

- Keep passwords secure and make sure they're not accessible to others.
- Comply with the school's password protocols.
- Do not share passwords.
- Do not use automated log on processes to store passwords.

Computers

- Lock your computer if it is unattended.
- Store removable drives securely e.g. USB memory sticks.

Software

- Only download new software from the internet if consent has been given.

Removing data from school

- Data taken off site must be secured at all times.
- Ensure you have permission to remove hard copy or digital information to work on away from school.
- If data is out of school overnight, it must be stored securely and not in a locked car.

Mobile devices

- Memory sticks, mobile phones, laptops and tablets must be encrypted.
- Only use personal devices at work if permission has been given and ensure school protocols are followed.

Sharing Data

- Do not share personal data without following the proper procedures and ensuring consent is given.
- Be aware that those seeking information may use deception to gain access. Always verify the identity of the data subject and the legitimacy of the request.

Accessing Data

- Do not access another employee's records without authority as this will be treated as gross misconduct and it is a criminal offence.

General

- Familiarise yourself with the school's key data protection policies and processes.
- If you think you have had a data breach, contact your Data Protection Officer/Named Individual immediately.

Treat everyone's data in the same way you would like others to treat yours!