



Data Protection: Ways of Working Guidance

Document date: June 2022



Together, pursuing life in all its fullness

Version	Date	Author	Changes
v1.0	June 2020	P. Blenkinsopp	Initial Issue
V1.1	June 2022	P. Blenkinsopp / L. Beale	Minor amendments plus addition of section 3.3

Review frequency	3 years
Review date	June 2025
Ratified by	Trust Leadership Team
Date of ratification	20 th June 2022
Lead/owner	Head of Operation and Compliance
Target audience	All staff
Document reference	POL-DP12

The electronic version is the definitive version of this document.

CONTENTS:

- 1 Introduction
- 2 Sending Emails
- 3 Sending Attachments
- 4 Emails to Multiple Individuals
- 5 Managing Emails
- 6 Password protecting documents
- 7 Using and Deleting Data
- 8 Paper Documents
- 9 Your Responsibilities
- 10 How to Password Protect a Document in Office 365

1 Introduction

The Diocese of Coventry Multi Academy Trust (the Trust) is a data controller for the purposes of data protection laws. Throughout this document, references to 'we', 'our', 'us' or the Academy refer to the school as part of The Diocese of Coventry Multi Academy Trust.

The Data Protection Act and the GDPR are now well established and the 'ways of working' within this document are intended to help us to protect our pupils and staff data.

The Trust has lots of documents and guides to help with this, including a data protection policy, Sharepoint guidance, CCTV policy, etc. But it's a lot to read and understand, and so here is a quick guide on how to do day to day activities in a Data Protection safe way.

2 Sending Emails

- 1.1 If you are sending an email that includes anything about a person directly, remember that anyone can ask to see any emails that include any information about them, so just make sure you'd be happy for them to read it before sending.
- 1.2 If you are including any sensitive data or data concerning more than one person then it is best to send this in an attachment as this is more secure. The data should be put it into a password protected document (see section 9 on how to password protect a document). and attached to the email. Please don't cut and paste the content from a document into the body of an email as this isn't secure.
- 1.3 If you are sharing lots of personal data, don't do this via email. Use data sharing folders or a Secure FTP (file transfer solution) if sharing externally. Password Protect the files if you wish to restrict access further (see section 9 on how to password protect a document).

2 Sending Attachments

- 2.1 Sending personal data as an attachment internally is OK provided you remember to password protect it. You should never send an attachment with personal data on it that isn't password protected. That way, if you accidentally send it to the wrong person, they can't easily open it. Keep in mind that password protection is not the same as encryption and it doesn't

mean the data is secure. However, you don't need to password protect things that you save on internal drives.

3 Emails to Multiple Individuals

- 3.1 The email system allows you to send the same email to a number of people at the same time using the CC (Carbon Copy) function. Unfortunately, this can be a really great way to cause a data breach. Someone's email address is their personal data so if you share it without their permission you might be breaking the law. For that reason, you should never use the 'CC' function when communicating via email.
- 3.2 If you need to communicate with multiple individuals then you should always use the 'BCC' (Blind Copy) function. This ensures that individual email addresses cannot be seen by the people receiving the email.
- 3.3 One of the biggest sources of data breaches in the trust has been emails sent to groups of parents, therefore this is no longer permitted. Instead use a messaging platform such as ParentPay or via the PrimarySite website.

4 Managing Emails

- 4.1 You should have no emails in your inbox, sent items, or folders that are more than 2 years old and they are therefore deleted automatically. Furthermore, you should be comfortable that all information in your inbox, sent folder and other folders needs to be there.
- 4.2 An easy way to control your sent items is to move an email you want to keep into a folder straight away. Then once a week, delete all your sent items.

5 Password Protecting Documents

- 5.1 To avoid trying to remember your passwords, here's a handy way of working:
 - 5.1.1 Save your document including data in the normal way to the normal place.
 - 5.1.2 Re-save and add the word "protected" to the end of the title and add a password to the document to open

it (see section 9 on how to password protect a document).

- 5.1.3 Send this password protected email on to someone – NEVER give the password via email!
- 5.1.4 Text, call or Teams message the person to give them the password.
- 5.1.5 You should then delete the password protected document from your folder straight away as you no longer need it.

6 Using and Deleting Data

- 6.1 Only use, save, and send personal data that is actually needed. Even if you follow all the principles in this document, you can still breach the data protection laws if the attachment you send has an address in it when the address won't be needed, etc. One of the most basic principles of data protection is that you should only collect the personal data that you need.
- 6.2 Our data retention schedule outlines how long we should keep personal data. The period varies depending on the types of personal data so you should ensure that you check this document regularly.
- 6.3 We need everyone to follow this schedule in their personal and shared folders. If you hold files containing any personal data, they need to be deleted in line with our data retention schedule.
- 6.4 We can't defend the retention of personal data that we don't need.

7 Paper Documents

- 7.1 It is best to avoid keeping paper documents containing personal data. However, this is not always practical in a school environment so if you need to retain paper documents they should be locked away when not required.
- 7.2 Use confidential waste bins or a shredder for personal data disposal. Please don't throw documents containing personal data into a normal bin or recycling bin where someone could get them back out.

8 Your Responsibilities

- 8.1 As a Trust, we are committed to handling and processing personal data correctly. As an individual, if you are trusted with the use of personal data, it's your responsibility to take care of it.
- 8.2 Following the guidance in this document will help you take care of personal data in a secure way.

9 How to Password Protect a Document in Office 365

- Click the **File** tab.
- Click **Info**.
- Click **Protect Document**, and then click **Encrypt with Password**.
- In the **Encrypt Document** box, type a **password**, and then click **OK**.
- In the **Confirm Password** box, type the **password** again, and then click **OK**.

