Microsoft Pilot - User Guidance

Information Security and Data Protection

As you begin your journey with Microsoft 365, here are a few things to consider and some hints and tips to get you started.

The approach to security and data management does not change between systems and Microsoft uses the latest security technology to ensure compliance and information security standards are met. It's essential that you understand your responsibilities for looking after information.

How you can work within the compliance framework has not changed with the new technology, but in some cases, it's good to understand how the new tools support us with this.

Confidentiality, Integrity & Availability (CIA)

We would like to share with you the security principles that are viewed as the primary goal and objective of a secure infrastructure.

When it comes to managing data in our systems, whether it's Microsoft 365, Content Server or any other system these are the principles apply:

- Confidentiality means that authorised people who need to see data, work with it, and those who are not authorized can't see or to be aware of them.
- Integrity means we protect data from being manipulated by an unauthorised party, whether it's at rest or in transit.
- Availability means ensuring that data is available to those who are authorised to see and work with it.

Data Classifications

When we are saving or sharing documents we need to consider the sensitivity of the information; who needs to see it and what protection we need to consider when sharing. As outlined in our Data Protection Policy.

Sharing Information

Barnardo's has an obligation to safeguard its staff, supporters and service users. Due to the sensitive nature of Barnardo's work, situations will arise where personal data will need to be shared with authorities and other agencies in order to protect individuals and resolve disputes and to ensure cohesive working. As outlined here Data protection: jargon buster | Inside Barnardos.

How to use the technology

How we store our data when using Microsoft

If you're working on a file by yourself, save it to OneDrive. Your OneDrive files are private unless you share them with others. This is similar to Google Drive. However, If you're working as a team you should continue using the Content Server where your team works.

All documents stored on your Desktop, and in your Documents and Pictures folders will be automatically synced to OneDrive and be retained on both locations.

All documents and data stored in G-Drive, can be copied across to OneDrive and automatically converted to Microsoft core formats - e.g. Google Doc becomes MS Word, etc. The conversion doesn't remove embedded links, however, if links are referring to a document on G-Drive which has been removed, they need to get updated as they would not work.

NOTE: Prepare and consider the impact on any live documents you are working with before you choose to move your documents across to OneDrive. Contact the Pilot Service Desk to get support in the transition.

NOTE: All documents on G-Drive should be purged before the end of March 2021.

How we share Documents in Microsoft 365

Microsoft 365 allows you to share documents within and outside Barnardos and allows you to set permission on what access/ edit rights etc they can have to the document.

Guidance: There are different ways of doing this and this link will provide you with user guides. Share your documents - Office Support (microsoft.com)

NOTE: Although there are no technology restrictions to share documents with individuals/organisations whether they use Microsoft or not, you still need to be mindful of data protection as outlined in our Data Protection policy.

NOTE: Consider the documents you are sharing, is it a single document or are you sharing a whole tier of data, does the person you are sharing with have the right to see other documents you may have stored in that tier?

Secure email in Microsoft 365

If an email contains sensitive personal data as outlined in Barnardo's Data protection: jargon buster, it is essential that the email is encrypted before being sent out. Microsoft 365 uses S/MIME encryption, which is an industry standard encryption type.

Guidance: To encrypt a message; In your new Email, go to the Options and from there you can select to encrypt your message. For step by step instruction follow this link.

Who to contact if you need further help and support

Technical & Guidance Query	Data protection and Privacy Query	Security Query
Workplace Office 365 Support Centre	Data Protection Team	Information Security Officer
Pilot Service Desk Email	Data Protection Officer	Technology Transformation Architect team
020 8498 7777		

Associated guidance and documents

Information Security Policy	Data Protection Policy
IT code of conduct	Data protection: jargon buster

Document History

Version	Date	Author	Status	Comment
0.1	04-12-2020	Cathy Diver and Matt Abbasi	Draft	This document is drafted for MS Pilot users
0.2	08-12-2020	Matt Abbasi	Draft	Associated guidance and document history added
1.0	08-01-2021	Cathy Diver	Final	Definitive Version

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA18) give individuals' certain rights regarding their personal data and how it can be shared. Failure to comply with these legal obligations could result in a loss of trust from the public and material fines from the ICO.