Information Security Guide for Beacon System Users, Plus…

Introduction

This information security guide aims to help minimize related security errors. It is essential to be aware of security threats that could affect Maghull & Lydiate U3A (the "U3A"). It is absolutely crucial that everyone using our Beacon Management System, both system managers and members, **have sufficient industry standard (for domestic users) security software in place to protect the system from cyber attacks** which ultimately could affect the whole National Beacon Infrastructure.

Scope of this Guidance

This guidance applies to the work of the U3A Beacon Team (the "Team") in particular but also, where appropriate, to **anyone accessing the U3A Beacon System both internally or externally**, (this guidance should also be considered when using the U3A website) which is deemed to be good practice.

The guidance also sets out the requirements that the Team has for personal information for: Team management purposes, for the delivery of the U3A Beacon Service and when processing personal data on behalf of U3A members. The guidance is reviewed on an ongoing basis by the Site Administrator to ensure that the Team is compliant.

This guidance is effective from **7th September 2021** and should be read in conjunction with the U3A Data Protection & Privacy Policy which details how personal information is gathered, stored and managed in line with data protection principles and the General Data Protection Regulations.

Accountability and Governance

The Committee has overall responsibility for the management and control of the U3A Beacon Management System. The Site Administrator is responsible for ensuring that the Team remains compliant with data protection requirements and can evidence that it has. They shall ensure that new members joining the Team receive an induction into how data protection is managed within the Team.

All Team members shall confirm agreement with this guidance document annually. **The Site Administrator shall review what data is held, its protection and manage/record who has access to it by monitoring Beacon use through the Audit Logs and Email delivery reports**. The Site Administrator shall also stay up to date with Data protection guidance and practice within the U3A movement.

Secure Processing

The Data Controller as defined in the M&L U3A Data Protection & Privacy Policy has responsibility to ensure that data is both securely held and processed. Data handling shall follow documented processes. These will include but are not limited to:

- Team members using strong passwords.
- Team members not sharing passwords.
- Restricting access of sharing member information to those on the Team who need to communicate with data subjects on a regular basis.
- Using password protection on laptops and PCs that contain or access personal information.

- Using password protection or secure cloud systems when sharing data between Team members.
- Ensuring firewall security on Team members' laptops or other devices.

Where Team members have responsibility for processing personal data, they shall:

- Use password protected files when sending data via email, i.e.: send two emails one containing the password protected data the second email containing the password(s).
- Not copying data files onto memory sticks
- Delete all relevant data files, including where attached to emails, from all devices once an issue is complete.

Personal data shall not be shared outside of the Team unless with prior consent of the Site Administrator and/or for specific agreed and documented reasons.

Access to Beacon Systems and Services

Use **strong passwords** for all accounts — at least 8 characters long and including special characters and numerals but containing no words in the dictionary. Attackers can brute-force guess simple passwords easily.

Create a unique password for every account. If you **reuse passwords**, then a leak in one service could compromise the others.

Keep passwords secret, without exception. Do not write them down for public view, do not save them in an unprotected file, and do not share them with colleagues. A random visitor or a disgruntled colleague could use your password to harm the organisation, an obvious danger, but the possibilities for damage are practically limitless.

Enable **two-factor authentication** for every service that allows it. Using 2FA helps prevent an attacker from gaining access to the service even in the event of a password leak.

Personal Data

Shred documents for disposal instead of simply throwing them away. **Personally identifiable information** in a waste bin guarantees attention from regulators and hefty fines.

Use secure channels to exchange files containing personal data (for example, share Google Doc documents with specific colleagues, not via “anyone with the link” option). Google, for example, indexes documents that anyone on the internet can view, meaning they can appear in search results. Emailed documents must be password protected with the relevant password being sent in a separate email.

Share members’ personal data with colleagues on a strict need-to-know basis. Beyond causing trouble with regulators, sharing data increases the risk of data leakage.

System Requirements

PERMITTED DEVICES/OPERATING SYSTEMS

To protect operating systems the following should be used. iPhones/iPads running iOS 11 or later, or Android devices running Android 10 or later, or Laptops and Desktops running Windows 10 or later or macOS 11 or later. Browsers should run the latest versions of Chrome, Firefox, Edge or

Safari. For security reasons iOS devices which have been "jailbroken" or Android devices which have been "rooted" should not be used, as doing so bypasses many of the security functions built into these mobile operating systems.

SECURITY SOFTWARE

Ensure that your devices have up to date Internet Security and Anti-Malware software installed.

SECURITY CONFIGURATION

All devices should be configured to provide basic security. As a minimum a device should be configured to lock itself after a few minutes if it is not being used. It must then require a password, PIN, or biometric such as a fingerprint before it can be unlocked using a strong password or PIN.

PATCHES AND UPDATES

Security patches and updates to applications and operating systems are often designed to close known security vulnerabilities which hackers can exploit to take over devices and networks. Please ensure that you update your applications and install operating system updates as soon as possible.

Data Ownership

It is important that you acknowledge that charity data stored on your devices belongs to the charity and not to the device owner. That means that if you step-down from your role, you agree that any charity data must be deleted from the device or returned.

Common Cyber-threats

Check links in e-mails carefully before clicking and remember that a convincing sender name is no guarantee of authenticity. Among cybercriminals' many tricks are used for getting people to click on phishing links, they may tailor messages to our U3A specifically or even use a member's **hijacked account**.

For finance managers: Never transfer money to unknown accounts solely based on an e-mail or direct message. Instead, directly contact the person who supposedly authorized the transfer to confirm it.

Leave **unknown flash drives** alone; don't connect found media to a computer. Attacks through infected flash drives are not just the stuff of science fiction — cybercriminals can and have planted malicious devices in public and in offices.

Before opening a file, check to make sure it is not executable (attackers often disguise malicious files as office documents). Do not open and run executable files from untrusted sources.

Emergency Contacts

Who to contact — please contact the Beacon Site Administrator, Chair of the U3A or any Member of Committee immediately — in cases of suspicious e-mail, weird computer behaviour, a ransomware note, or any other questionable issues.