Beacon Team – Protecting U3As' Data

Background

The Beacon Team delivers Beacon as a service to U3As on behalf of the Third Age Trust and must therefore comply with Trust and Beacon Team Data Protection and Privacy Policies.

The Beacon Team is required to handle U3As' data as part of the migration, support and technical investigation processes.

Purpose

The purpose of this document is to define the procedures that Beacon Team members must adopt when:

- supporting U3As in preparing their data
- checking the data in preparation for migration
- handling the data during migration
- accessing the U3A's data on Beacon to confirm the success of migration
- supporting the U3A during their initial configuration of their Beacon site
- investigating technical problems

General

Throughout, Beacon Team members must insist that U3As who are supplying data use password protection on data files, and to transmit the password by separate email.

There is no requirement to explicitly confirm to a U3A that copies of their data have been deleted in accordance with this process.

When presenting/demonstrating Beacon, the Demoton instance should be used, and the presenter's 'home' U3A's data must not be used.

Supporting the U3A in preparing its data

Any copies of the U3A's data should be deleted from the Team member's computer (including any sent/received by email) within 30 days of the data being submitted for migration.

Checking the data in preparation for migration

Any copies of the U3A's data should be deleted from the Team member's computer (including any sent/received by email) within 30 days of the data being submitted for migration.

The U3A should be provided with any changed data files, so that they own the final data to be migrated, and they send their own data to the Support Team for migration.

Handling the data during migration

Any copies of the U3A's data should be deleted from the Team member's computer (including any sent/received by email) within 30 days of the data being successfully migrated.

The migration team should reject any data that has not come from the U3A's nominated contact.

If data in the U3A's submitted file is altered to achieve a successful migration, the amended data workbook/spreadsheet should be returned (password protected) to the U3A.

Accessing the U3A's data on Beacon to confirm the success of migration

Access to the U3A's Beacon site should be solely to confirm the success of migration.

No data should be extracted (e.g. downloaded) from the U3A's Beacon site.

Supporting the U3A during their initial configuration and subsequent support of their Beacon site

Access to the U3A's Beacon site by a Superuser should only be on request from the U3A and should be solely to assist the U3A with their issue.

If the U3A provides a login to their Beacon site for use by a team member, then the access should be solely to assist the U3A with their issue, and the U3A should be asked by the team member to remove the login on completion of the support task.

If data must be extracted (eg downloaded) from the U3A's Beacon site to deliver the support task, then it should be immediately deleted from the Support Team member's computer on completion of the support task.

It is recognised that, as part of overall system maintenance, the Team may inspect system and email logs which may contain personal data such as usernames or email addresses.

Document Revisions

Rev	Date	Author	Description
0d1	4/3/18	A Stanfield	Initial draft
0d2	6/3/18	A Stanfield	Actions added
0e	14/3/18	A Topp	Background, General, Purpose
0f	17/3/18	A Stanfield	Minor edits
0g	31/3/18	A Stanfield	Changes references from Support Team to Team
1	31/3/18	A Topp	Issued as pdf