Ely & District u3a Information Technology (IT) Security Policy

Purpose

The purpose of this document is to describe the main vulnerabilities of Ely & District u3a (Ely u3a) use of Information Technology (IT). It also describes how these identified vulnerabilities are managed.

Use of IT

Our Website

The information on our website is not especially vulnerable or critical. Only trained users are allowed to edit the information and normally their access is restricted to their areas of interest. Access is via a username and a password that is personal to the user.

The data of possible use to hackers held by the website are the names, email addresses and similar details of page editors and, in some cases, group leaders. Our bank account details (account name, sort code and number) are also openly available in documents linked to the website.

If the information on the website was destroyed or lost it would not be overly critical because the website information is regularly backed up.

Our Membership Database (Beacon)

Access to Beacon is via a username and a password that is personal to the user. Only trained users are allowed to edit the information and normally they are restricted to their areas of interest.

If Beacon was hacked then:

- The personal details of our membership could be stolen.
- The database integrity could be compromised. Beacon is regularly backed up.

The security of Beacon is managed by National u3a.

The Members' Portal and Online Member Joining

Access to the members' portal is via a username (email address) and a password personal to the user.

The members' portal enables individual members to amend their user records within Beacon. They can also use PayPal or a credit/ debit card to pay for their membership renewal. As far as we can tell, we think Beacon does not store members' bank details, it only uses them for each transaction made.

The security of Beacon is managed by National u3a.

Our Bank Accounts

Access to our bank accounts is restricted to officers of Ely u3a and on an “as required” basis. Access is via a username and a personal password.

The security of our bank accounts is managed by our bank.

Our Members’ Email Accounts

Ely u3a makes extensive use of email to communicate with its members. Individual members are responsible for the security of their email accounts. At present, up to about 5 member email accounts are hacked each year.

Ely u3a should regularly remind members that passwords should be strong (not simple, not information available on social media accounts). All members should be cautious when responding to un-solicited emails, texts or telephone calls.

The following text is proposed for inclusion in the Ely u3a Newsletter 3 or 4 times per year.

IT Security

Like many other organisations, Ely & District u3a makes extensive use of Information Technology (IT). Our main vulnerability is to hackers who either guess passwords (e.g. from social media) or trick members into revealing them (e.g. by clicking links in un-solicited emails or texts) or during cold telephone calls.

Please ensure your passwords are strong and not easily guessed.

Please by vigilant when responding to un-solicited emails, texts or telephone calls. Be extra wary of any of these which state or imply urgency.

Up to about 5 members of Ely & District u3a each year have their email accounts hacked. Please ensure it is not you.