CYBER SECURITY POLICY

Purpose

Bavs is committed to protecting the personal data that it processes; and protecting the integrity of its networks and IT equipment. This policy sets out the steps it will take to meet these commitments.

Scope

The policy applies to all IT equipment and networks used by Bavs, whether owned, leased or covered by a subscription. It also applies where stated, to any private equipment that is used by staff and/or volunteers for Bavs purposes.

Data use and storage

Personal data will be used in accordance with our data protection policy and associated privacy policy.

All data processed by Bavs will be used and stored as follows:

- No personal data shall be left unattended on any desks or tables. Visitors must be signed-in and their time of exit noted.

- Data will be stored in a cloud-based system. Once personal data has been transferred to this system, hard copies of any data collection forms and/or notes will be stored securely in a lockable filing cabinet, or alternatively they will be shredded.

Protection from malware

Bavs will take the following measures to prevent malware contamination:

- Anti-malware software will be installed across the Bavs network on all Bavs devices.

- Administrator-only permissions will be set for installing new apps and software. Staff and volunteers should not download third party apps and software from unknown or untrusted sources.

- Operating systems of computers, smartphones and tablets will be updated whenever the provider releases a new security update.

- Operating system firewall's will be enabled in addition to network firewalls. Network security will be monitored and updated as required.

Email Safety

Staff and volunteers will be trained to spot unusual, suspicious or bogus emails; and to draw these immediately to the attention of colleagues. Any accidental opening of such emails and/or links within the message should be reported to the chief officer for consideration. Depending upon the nature of the intended scam, the matter may also be reported to the police.

Internet Safety

Email, internet and social networking is covered in the Bavs staff handbook. In addition, Bavs will take the following steps to promote Internet Safety:

- Staff and volunteers should not use the Bavs network, or any Bavs device, to access shopping, gaming, or gambling websites, or for the purpose of purchasing subscriptions, without the express permission of the chief officer.

- Only legitimate work-related documents should be downloaded over the Bavs network or onto Bavs devices.

- The downloading of applications will be restricted to network administrators only; and will not be downloaded from unknown third party websites.

- If on Bavs business, staff and volunteers should not engage online with Internet trolls, including when using their own devices.

- The accidental opening of any suspicious or bogus website; or of any site that appears to be promoting unlawful activities, should be reported to the chief officer.

Password Policy

The following steps should be taken to ensure the integrity of passwords:

- All default manufacturer passwords or codes on IT equipment used for Bavs purposes, including personal devices, will be changed to something suitably robust.

- Individual user passwords shall be used by all staff or volunteers for any local and online accounts accessed by staff or volunteers. In addition, accounts that process personal data, will, where available, use two-factor authentication.

- All passwords must be robust. For example, this could be three randomly unconnected words and/or a combination of upper and lower case letters, numbers and symbols.

- Bavs will store passwords for users in a digital password manager, accessible only by two nominated members of staff. The master password for this will be changed whenever any of the nominated individuals change. Alternatively, users should keep details of passwords in a secure place, such as a locked filing cabinet.

Laptops

Any laptop used for Bavs purposes, or that connects to the Bavs network, should be protected in accordance with our password policy (above).

Where personal data used by Bavs is stored on a laptop, that device will be encrypted using suitable software or the operating systems in-built encryption.

Users should avoid connecting their laptop to a public Wi-Fi and instead tether their laptop to a mobile phone connected to a data network such as 4G.

Smartphones and tablets

Bavs devices, or any personal device used for Bavs purposes, should be protected as follows:

- Where applicable, devices should be protected by a six-figure, rather than a four-figure passcode.

- Where applicable, users should switch on fingerprint of face identification.

- Users should enable location tracking, remotes access lock, and remote erasure of data

- The latest releases of iOS or Android operating systems should be installed

- Apps should be updated when new versions are released.

- Users should avoid connecting to public Wi-Fi and instead connect to a mobile data network (such as 4G).

Training and supervision

All staff and volunteers will be

- trained supervised in the appropriate use of IT devices, software applications and relevant policies?

- made aware of Bavs cyber security measures and their importance, including the relationship to data protection law?

- trained on how to report a cyber or data breach; and where Bavs believes it has been the subject of cyber fraud and/or a data security breach, the procedure set out on our Data Protection Policy will apply.

Produced by: Bavs/DG

Agreed: 16 June 2021 Review date: June 2024