Bring Your Own Device (BYOD) Policy

Bring your own device (BYOD) is the practice of allowing staff to use their own devices in the workplace and to use those devices to securely access the organisation's systems, applications and information. This can mean using their own smartphones, tablets or laptops for work.

This policy is intended to protect the security and integrity of Lightyear Foundation's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. Lightyear Foundation employees or freelance staff must agree to the terms and conditions in this policy in order to be able to connect their devices to the charity network.

Scope

This policy applies to all staff, freelancers and authorised third parties of the organisation who use BYOD. The BYOD service includes a range of systems and access may vary by individual depending on the requirements of individual roles.

This policy is in place to make sure:

- BYOD systems and data are used appropriately, legally and securely.
- personal devices are used in a way which protects confidentiality in accordance with GDPR.
- staff clearly understand their responsibilities when using BYOD.

Acceptable use

- The charity defines acceptable use as activities that directly or indirectly support the objectives of Lightyear Foundation.
- Staff should never try to access systems for which they are not authorised.
- Confidential data should only be accessed for a specific work-related requirement.
- Any suspected breach must be immediately reported.
- Devices may not be used at any time to:
    - store or transmit illicit materials.
    - store or transmit proprietary information belonging to another organisation.
    - harass others.

Devices and support

- BYOD will only be supported on devices which can run the latest version of Apple or Android operating systems.
- Staff will be expected to make sure their devices are kept updated or risk losing access to some systems.
- Connectivity and access issues are supported as best as possible by the charity's IT support volunteers.
- Connectivity by Wi-Fi or mobile data contracts will be the responsibility of the device owner.

Security

- Use of a device that has access to work systems by BYOD should be limited to its owner and must not be shared.
- Staff should always keep their account login details, passwords and PINs confidential and never share them with anyone.

- Staff should be conscious of the setting in which devices are being operated and should ensure data and systems displayed are not visible to others. Data accessed must not be saved to the device or copied off it. Screenshots of systems must not be taken.
- Staff must immediately inform Lightyear Foundation if:
    - their password has been breached
    - their device gets lost or stolen
    - organisational systems are not working normally
- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the charity network.
- The charity's strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords should be rotated every 90 days and the new password can't be one of 5 previous passwords.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Employees' access to charity data is limited based on user profiles defined by the CEO and Board of Trustees and automatically enforced.

Costs

- Staff are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD.
- Staff are responsible for all mobile data or Wi-Fi hotspot costs related to BYOD usage and should monitor these to ensure they have sufficient allowance.

Risks/Liabilities/Disclaimers

- The organisation will not accept any liability for loss or damage of personal devices that are using the BYOD system.
- Staff should inform Lightyear Foundation immediately if they lose their personal device or have it stolen.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the charity's acceptable use policy as outlined above.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of charity and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Where operating systems are found to be out of date the staff member will be informed and expected to upgrade to the most current version within 7 days.
- Lightyear Foundation reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Last reviewed: 30/09/2023