BEYONDLY

**G-8**

# Information Security

## Policy Statement

Beyondly exists to lead, inspire and educate to positively impact society and the environment. In the day-to-day operation of its business, the company has access to – and is required to store – data and information relating to employees, customers, partners, and suppliers.

Beyondly is committed to preserving the confidentiality, integrity and availability of information. All employees, partners, and suppliers have a responsibility to adhere to this Information Security (IS) policy at all times.

For the purpose of this IS policy, employees, suppliers and partners are referred to as parties of Beyondly.

## Acceptable Use

### Access

In order to perform their job function, supply agreement, or partnership responsibilities, all parties have a requirement for some level of access to the systems used by Beyondly. The level of access granted is appropriate to ensure all tasks/responsibilities can be completed.

### Use of monitoring of systems and resources

All parties have a responsibility to use the systems, resources and assets provided by Beyondly in an appropriate manner and only for a legitimate business purpose. All systems, resources and assets provided by Beyondly remain the property of Beyondly.

The Company reserves the right to monitor employees' emails, telephone communications and internet usage but will endeavour to inform an affected employee when this is to happen and the reasons for it. In instances where the employee has left the business, then Beyondly reserve the right to access any of these communications as part of investigations, audits etc. The Company considers that valid reasons for monitoring an employee's email and internet usage include suspicions that the employee has:

- been spending an excessive amount of time viewing websites or sending emails that are not work-related; or
- acted in a way that damages the reputation of the Company and/or breaches commercial confidentiality.

BEYOND TODAY ↘ TOWARDS TOMORROW ↗

If the Company monitors employees' email and/or internet usage to ensure that it is in accordance with this policy, access to the web may be withdrawn in any case of misuse of this facility.

If appropriate, disciplinary action may also be taken in line with the Company's Disciplinary Policy (E-8).

For the purpose of this IS policy, systems, resources and assets is defined as, but not limited to:

- Desktop and laptop computers
- Desktop phones
- Work mobile phones
- Removeable media (such as USB drives and portable hard drives)
- Any other physical hardware provided by Beyondly
- Licences for applications made available throughout employment, supply to, or partnership with Beyondly and any user accounts associated with these licences/applications

There should be no expectation of privacy for any information stored or transferred on any system, resource, or asset provided by Beyondly - with the exception of private and/or sensitive information, which will be handled securely in line with the company's GDPR and privacy policies.

Beyondly and all its parties have a responsibility to monitor and maintain the systems and resources provided and ensure that they remain fit for purpose. Employees should raise any concerns with their line manager, senior management, or IT staff. Suppliers and partners should raise any concerns with their point of contact at Beyondly.

**Installing and Updating Software**

All parties should not update or install software that may impact information security without first checking with relevant IT staff. Software should only be installed if it is included on the approved software and apps list (found in the applications tab at https://portal.beyond.ly/admin/systems/equipment/) which is reviewed on a quarterly basis by the Systems Team and communicated to employees during induction and in line with any changes made. It should also be installed from verified/trusted/known publishers and from known/reputable sources (for example, Microsoft apps should only be downloaded from Microsoft, and not a third-party website). Parties should be aware that vulnerabilities in software can be introduced intentionally (malicious software [malware]) or unintentionally (a bug).
Reputable software publishers will work to address any vulnerabilities in their software by periodically releasing updates or patches. Software should have automatic updates enabled where possible to take advantage of this. Where automatic updates are not possible or practical, any instance of a program informing the user that an update is required should be brought to the attention of the systems team unless advised otherwise.
Many programs require a full or partial system restart to apply updates. Therefore, all devices used for company purposes should be fully restarted at least once every two weeks.

**Shared Files**

Beyondly provides employees with access to a shared network drive. Employees are to save files in the relevant folders as per the shared drive governance document.

Any personal, sensitive or confidential files should be saved locally on an employee's machine. Employees should be aware that the majority of files saved locally on their machine (particularly those in the Desktop and Documents directories) are also saved on the server, but in a password protected directory. Access to these files is only granted for an authorised user.

**Encryption software**

No party should encrypt (password protect) directories and/or files without first discussing with senior management or IT staff. If not managed properly, encryption can result in directories and/or files being locked and difficult to recover.

**Chat GPT**

Chat GPT is an AI language model which can be beneficial to the business to use in terms of productivity and efficiency. Employees are authorised to use Chat GPT for work related purposes whilst adhering to the terms of this Information Security policy. For clarity by using Chat GPT employees agree to abide by the following:

- Not disclose any confidential, financial, sensitive or customer information to Chat GPT
- Be responsible for maintaining security of their login details
- Be responsible for checking the accuracy of any output from Chat GPT
- Report any suspicious activity or security issues to the systems team immediately
- Not use Chat GPT for any activities which contravene any other of our business policies or applicable laws

## Confidential Data

It is the responsibility of Beyondly to define the meaning of confidential data. This has been determined as follows:

- Employee information including but not limited to, personal data, sensitive personal data, and criminal record data (as defined in the Data Protection and GDPR Policy)
- Customer, supplier, and partner information including but not limited to, communications, contact details, data submissions, and data files
- Company information including but not limited to, financial information, pricing structures and management direction

Consideration should be given to any new data or information as to whether it meets the definition of confidential data.

**Handling confidential data**

All confidential data should be handled securely and not shared with any third parties without prior consent from Beyondly.

Any need for an individual to handle confidential data outside the functions outlined in their job description, supply agreement, or partnership responsibilities should be discussed with their line manager or senior management, or otherwise point of contact at Beyondly.

Confidentiality and non-disclosure agreements may be used to protect confidential information.

## Network Access

All devices connected to the internet should be secured with a password, and – where possible – setup with antivirus software and a firewall and periodically scanned. This includes personal mobile devices.

Any device containing company information, and all gateway network equipment (e.g. wireless access points, routers, firewalls), should prevent inbound access via the use of the network address translation (NAT) service or a 'deny all' firewall rule. Where inbound access is required, a business case should be created and maintained which will document the reason for such access.

**Onsite/Office access**
Devices can be connected to the network either through a physical connection using an ethernet socket. (usually found in the plastic trim in the skirting around a wall or in a cover in the floor) or through a wireless connection to a router.

Any difficulty obtaining access to the network should be discussed with Beyondly's IT partner, A & N Business Computer Systems.

**Ethernet**

No party or individual shall remove or exchange any ethernet cable without having sought approval from IT staff. Other systems make use of the local area network (LAN) and only ports configured for PC use will allow proper access.

If properly configured, a machine connected via ethernet cable will have access to the internet and the shared drive.

**Wireless**

To gain access wirelessly, a party or individual will require the password/key. If this is not known, this information should be obtained from IT staff. Company laptops should be connected to "beyondly" and all other devices should be connected to "beyondly-guest"

Company issued laptops are the only devices to connect to the staff Wi-Fi network. All mobile devices and guest devices should connect to the guest Wi-Fi network, which does not have access to Beyondly's shared drive and network.

**Mobile devices**

Owing to the lack of mobile reception on the estate, it is common for individuals to connect personal mobile devices to the guest wifi network. Any personal mobile device connected to the network should only be used for a function that would also be appropriate on a Beyondly device. Individuals should take care when using mobile devices connected to the network and consider whether they would install/run an application or visit that webpage on a Beyondly device.

**Remote Access**

The network is configured to allow authorised remote access via the use of a Virtual Private Network (VPN).

Any device that needs to be configured to connect to the network remotely should be brought to the attention of IT staff.

All devices provided by Beyondly should be connected to the VPN when also connected to the internet, particularly when connected to the internet via a home network. This will ensure that any information transferred is secured. Ahead of homeworking, employees must provide details of their Wi-Fi network to ensure this

is safe. Employee's are to share details of their personal devices and home wifi which are to be reviewed on an annual basis to ensure they are safe.

To avoid increased security risks, when working remotely, employees should avoid using public Wi-Fi wherever possible. As an alternative, employees should connect via mobile hotspots, or use the company mobile Wi-Fi device (this will need credit adding to it in advance).

**Personal Devices - Employees only**

On occasion there is a requirement for employees to work from personal devices. The use of a personal device does not permit any deviation from any other part of this Information Security Policy during an employee's contracted working hours. Personal devices should be setup with an antivirus software and periodically scanned to assess vulnerabilities. Personal devices must be declared to the systems team before they are to begin use for work purposes. This does not apply for multifactor authentication apps, other apps that do not store company data or device default texting and calling apps.

## Passwords

Passwords should conform to the guidelines below:

- No password should be saved or transferred as plain text without any additional verification/encryption preventing unauthorised access.
- No password should be written down and stored near the device the password provides access to.
- No password should be saved and stored using browser password storage systems.
- No password should be saved to shared devices under any circumstances.
- If the site/system allows it, a party or individual should provide additional recovery options such as email or text verification codes.
- Passwords should not be duplicated (using the same password for multiple sites/systems).

*Employees only:*

The use of LastPass is required as the primary storage point for passwords. Any new passwords (excluding network login and your LastPass master password) should be created using the password generator. Passwords shared between employees should be done using LastPass to mitigate against the risk of insecure storage and/or transfer.

If a password is believed to be compromised it must be changed immediately, without exception. If it is unclear how to do this in any case, contact the systems team. In addition to any security incident you would be immediately aware of, it is also advisable to check the security dashboard in LastPass regularly as it will report any security incidents it finds.

## Making Payments

All parties should have a secure payment process in place. This should include requesting and receiving bank details in appropriate formats (for instance: on company letter headed paper and signed by a director as listed on Companies House, a copy of a blank cheque, bank statement or paying in slip). Any changes in bank details should be confirmed verbally using a trusted contact number prior to any requested updates.

Relevant training should be conducted for any staff with the authority to input and authorise payments, and at regular intervals, to ensure they are aware and adhering to all cyber and fraud prevention precautions and are aware on how to report such issues. All training and resources should also be reviewed annually to ensure they are fit for purpose and in line with best practises.

## Information Transfer

All parties should be aware of the different methods of transferring information and the best practises for each to minimise the risk of accidentally leaking information or providing information to an unintended recipient.

**Cyber Security/Awareness**

All individuals should undergo routine cyber security awareness training.

As much as possible, all login accounts that provide access to company information should be secured with an additional layer of authentication (multi-factor authentication).

**Electronic – Email**

All parties should be aware that phishing emails (emails impersonating another person - often another party) are commonplace. Caution should be used if there is any reason to suspect suspicious activity, particularly if there is an attached file or embedded link. No file or link should be opened or clicked if there is any reason to suspect suspicious activity. It is common for cyber criminals to impersonate senior members of staff - a director or person in a position of financial authority - to try and elicit a sense of importance or urgency along with a request. Where appropriate (particularly if the message is concerning a transfer of money or confidential data) attempts should be made to contact the supposed sender by another method of communication (face-to-face conversation or telephone call). If unsure, parties should highlight any potential phishing emails to IT staff.

The use of a disclaimer highlighting external emails to assist with identifying phishing attempts is recommended. All Beyondly emails have this measure in place.

All parties should take care when replying or forwarding emails to ensure that the content of the email thread is suitable for the intended recipients. Particular care should be taken when using ‘Reply All’, especially if the recipients of the email include both internal and external contacts, and/or if the recipients span numerous departments and job functions.

*Employees only:*
It is expected that fonts, colours, and signatures adhere to the company brand guidelines.

**Electronic – Teams**
Verification of coworkers’ identity is naturally integrated by means of the contacts list – outside communications happen less frequently and are much harder to spoof, so it is easier to discern any potential bad actors. Additionally, communications are encrypted, so it is a safe option for file transfer.

Beyondly employees are to log any phishing attempts onto the systems ‘Cyber Incident Log’ which is regularly monitored and used as part of internal training with the team,

**Electronic - Telephone**
Individuals should consider whether the information to be communicated is suitable for the answering recipient. For inbound calls, individuals should attempt to verify the caller before disclosing any confidential, sensitive or company information.

*Employees only:*

The phone system used by Beyondly is CallSwitch, which uses Voice over Internet Protocol (VoIP).

Employees should use the laptop or smartphone app to control the VoIP system to make business calls in all circumstances.

There is a requirement for many employees to have the VoIP system installed on personal devices. The use of a personal device does not permit any deviation from any other part of this Information Security Policy during an employee's contracted working hours. Outside an employee's contracted working hours, the VoIP system should be disabled on personal devices.

**Electronic - Cloud file storage (e.g. OneDrive)**

A cloud storage solution could be utilised if there is a requirement to share a file with between parties that is difficult to transfer via email because of the file size or type. Care should be taken to ensure appropriate sharing options/permissions for the file (view, edit, prevent download, etc.) are selected. It is recommended that the file is shared only with specific people and that editing is disabled, a password is set, and downloads are blocked - unless any of this functionality is explicitly required.

*Employees only:*

Employees each have a OneDrive account associated with their Office 365 licence. This is most easily accessed via internet browser but employees are welcome to set this up as a syncing folder on their Beyondly machine. Employees should bring this to the attention of IT staff if they wish to set this up and require assistance.

Files shared in Microsoft Teams Chats are automatically saved in OneDrive. Files shared in Channels in a Team are not saved in OneDrive and are instead uploaded to Microsoft SharePoint.

**Electronic - Cloud file storage (e.g. OneDrive)**

The use of web hosted file sharing sites such as WeTransfer is not prohibited, but it is recommended that parties explore the use of a cloud storage solution first.

If a web hosted file sharing site is required, parties should first check the security that the site offers and ensure that the site is based in the EU and have a GDPR statement/policy to ensure that they are compliant. Any uncertainty should be highlighted to IT staff.

WeTransfer is the recommended option.

**Physical**

There is often a requirement to transfer information physically, either on a USB drive or on a portable device (such as a laptop or mobile phone). Information carried on portable devices comes with an increased risk of loss or breach, owing to the fact the device has an increased chance of being lost or stolen.

**Physical - Removable Media (portable HDDs and USB drives)**

Removable media includes all information storage that be inserted and removed from a system. This includes but is not limited to: CDs, DVDs, USB drives, and portable hard drives.

All removable media containing company information should be encrypted to prevent information breach in the event that the drive is lost or stolen. Removable media should be encrypted using BitLocker. The encryption key is to be obtained from IT staff.

At end of life, all removable media should be formatted to ensure no confidential data can be recovered by any third party. Removable media should be disposed of correctly in line with applicable legislation.

*Employees only:*

USB drives are encrypted using BitLocker. The encryption key is to be obtained from IT staff. No employee is to encrypt a new USB drive without first having discussed with IT staff.

Beyondly provided USB drives should only be used to transfer company information. The use of personal USB drives should be avoided to mitigate against exposing the network to an infected file.

**Physical – Written Information**

Individuals should avoid transferring information on paper or other non-electrical medium. This information cannot be protected from unauthorised access should it be lost or stolen. In instances where physical sensitive information is received, it should be stored securely (preferably electronically) if needed and shredded following use.

**Physical – Devices**

All devices that contain or provide access to information should be password protected. Beyondly operates a 'clear screen' policy whereby no information or access to information is left unattended. Devices containing company information should be locked when an individual leaves their desk. Individuals should be aware of the keyboard shortcut to lock a Windows device: Windows Key + L.

All parties should avoid having non-essential business system applications on mobile devices (such as LastPass, Xero & Salesforce). Where an application is required, care should be taken to prevent unauthorised access by signing out of the application when it is not in regular use.

**Physical – Workstation (Desk)**

Beyondly operates a 'clear desk' policy. As much as reasonably possible, workstations should be free of confidential and/or sensitive information. Workstations should be tidy and organised to minimise the risk of loss and/or breach of information.

## Incident Response

Any incident or potential incident of information loss or breach should be highlighted immediately to senior management and IT staff at the soonest possible opportunity. This communication should include:

- The type of information – confidential or non-confidential
- Details of the information – if known
- Source/cause of the loss or breach – if known
- Any affected parties

All parties should ensure that they are familiar with the Business Continuity Policy and, where applicable, the Business Continuity Plan.

## Change Management

All business changes that may impact information security should be considered in line with this Information Security Policy. In particular, any change should be

evaluated to determine if the information affected by the change remains secure and/or if the change introduces any potential of loss or breach of information.

## End of Contract

At the end of the contract all confidential information stored on any device not owned by Beyondly must be destroyed or disposed of. No company information acquired during the duration of the contract can be used for any other purpose or shared with third parties. At the end of contract, Beyondly will retain any information it is legally required to do so, such as compliance and financial information.

Any systems, resources, or assets provided by Beyondly should be returned to Beyondly. Any access to systems granted through contract with Beyondly shall be revoked.

## Final Remarks

All elements of this IS Policy should be considered in project management, regardless of the type of project to be undertaken.

**Issue Number:** 5
**Issue Date:** 05 September 2023
**Issued by (Name):** Jessica Aldersley
**Issued by (Signature):**

**Position:** Director