GDPR
(General Data Protection Regulations) Policy

Document:	Issue:	Date Issued:	Review Date:	Review By:
BUK.SHEQ.PO.037	02	08/01/2022	07/01/2024	Nigel Johnson

CONTENTS

1. Purpose

The purpose of this Policy is to protect the confidentiality, integrity and availability of Barlows UK Ltd information systems by controlling access.

2. Scope

Desktop Computers
Email
Laptop Computers
Mobile Phones & tablets
Offsite storage
Paper Documents
Personal devices
Removable storage
Social Media
Verbal Communication

3. Policy Statement

Barlows UK Ltd information system resources are assets important to Barlows UK Ltd business and stakeholders. Its dependency on these assets demands that appropriate levels of security be instituted and maintained. At any given time, some of Barlows UK Ltd information resources will be held on paper, laptops, desktops, mobile devices (including smart phones), tablets and storage drives, which may be removed from Barlows UK Ltd premises. It is Barlows UK Ltd policy that appropriate access control measures are implemented to protect its information system resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

4. Policy Objectives

The objective of this policy with regard to the protection of information system resources against unauthorised access is to:

- Minimise the threat of accidental, unauthorised or inappropriate access to information owned by Barlows UK Ltd or temporarily entrusted to it.

- Minimise Barlows UK Ltd network exposure, which may result in a compromise of network integrity, availability and confidentiality of system information resources.

- Minimise reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach confidentiality.

4.1 Policy Review

Barlows UK Ltd information system resources are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Adequate precautions are required to prevent and detect unwanted access. Users should be made aware of the dangers of unauthorised access. Barlows UK Ltd have where appropriate, introduced special controls to detect and prevent such access.

4.2 Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an ongoing basis by Barlows UK Ltd. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of email or other relevant communication media. Users shall then have the obligation to obtain the current information system policies from Barlows UK Ltd intranet or other relevant communication media.

5. General

Laptops, Desktops, Paper, Removable Storage, Mobile Phones, Tablets, Verbal, Email, Offsite Storage, Personal Devices and Social Media are essential business tools, but they are vulnerable to theft of data. Any usage outside of Barlows UK Ltd premises increases the threat from people who do not work for Barlows UK Ltd and may not have its interests at heart.

Mobile devices are especially vulnerable to physical damage or loss, and theft- either from resale or for the information they contain.
The impacts of breaches of security involving Laptops, Desktops, Paper, Removable Storage, Mobile Phones, Tablets, Verbal Communication, Email, Offsite Storage, Personal Devices and Social Media include not just the replacement value of the hardware, but also the value of any data on

them or accessible through them. Information is a vital asset. Barlows UK Ltd depends very heavily on its information systems resources to provide complete and accurate business information when and where required. The impacts of unauthorised access or modification of critical or sensitive data will usually far outweigh the cost of the equipment itself. The right to be forgotten under GDPR is the right an individual has to be forgotten. Therefore Barlows UK Ltd employees are expected to ensure that all personal information is secured in a controlled and approved environment. Personal information may include name, date of birth, personal address, next of kin, phone numbers, email address, bank details, national insurance number, medical history, qualifications, disciplinary action and wages.

5.1 Encryption

Laptops, Removable Storage, Mobile Phones, Tablets, Offsite Storage and Personal Devices must be encrypted. Laptops that process Barlows UK Ltd system information resources MUST have full Deslock disk encryption. Company Passwords are subject to Barlows UK Ltd Password & Policy Guidance. If you have reason to believe that items are not password protected or your laptop is not Deslock protected, please contact Barlows UK Ltd IT department. All paper documents are subject to being confidentially destroyed by shredding as defined in Barlows UK Ltd Paper Destruction Guidance.

5.2 Access to on-line information

The following guidelines must be observed:

- The physical security of any Laptop, Removable storage, paperwork, Mobile Phones, Tablets, Offsite Storage & Personal Devices being used for business purposes is your personal responsibility and you must take all reasonable precautions. Be sensible and stay alert to the risks.
- Keep your Laptop, Removable Storage, Mobile Phones, Tablets, Offsite Storage & Personal Devices within your possession and within sight whenever possible, especially in busy public places such as restaurants & railway stations.
- Lock the Laptop, Removable Storage, Mobile Phones, Paperwork, Tablets, Documents, Notes, Offsite Storage & Personal Devices when out of sight or not using them. Never leave a Laptop, Removable Storage,

paper documents, Mobile Phone, Tablets or Personal Device visibly unattended in a vehicle. If necessary lock it out of sight.

- Carry and store Laptops, Removable Storage, Mobile Phones, Tablets & Personal Devices in protective covers to prevent the chance of accidental damage.

- Barlows UK Ltd maintains records of all Barlows UK Ltd owned IT equipment. If it is lost or stolen you can contact them for this information. It is your responsibility to notify the police immediately and inform Barlows UK Ltd GDPR team as soon as reasonable practicable.
- Viruses and malware are a major threat to the organization. Especially if anti- virus software is not kept up to date. The anti- virus software will update automatically as long as you are connected to the internet. If you have reason to believe that this is not happening please contact the IT department.
- Virus scans normally happen automatically, Barlows UK Ltd can inform you how to initiate manual scans if you wish.
- Respond immediately to any virus warning message on your computer and contact the IT department.
- Avoid opening any unexplained email attachments.
- Do not open any physical deliveries such as post or parcels which are not addressed to you.
- Avoid sending confidential personally identifiable information over any networks.
- You are personally accountable for all networks and systems accessed under your user ID, so keep your password secret.
- Laptops, Desktops, Removable Storage, Mobile Phones, Tablets, Offsite Storage & Personal Devices provided are for official use by authorised employees. Do not loan your device or allow it to be used by others such as family and friends.
- Avoid leaving Laptops, Desktops, Removable Storage, Mobile Phones, Tablets, Offsite storage & Personal Devices unattended whilst logged on. Always shut down, log off or activate a strong password protected screensaver before walking away from the device.
- The contents of Laptops, Desktops, Removable Storage, paper documents, Mobile Phones, Tablets, Offsite Storage & Personal Device screens could be easily observed by someone sitting in close proximity. Please ensure that no sensitive or critical information can be viewed by an authorised person when using a Laptop, Desktop, Removable Storage, Mobile Phone, Tablet, Offsite Storage or Personal Device in any location. Be particularly vigilant in public places such as trains.

5.3 Policies

Laptops, Desktops, Removable Storage, Mobile Phones, Tablets, documents, Offsite Storage & Personal Devices are subject to Barlows UK Ltd full range of policies. Please ensure that you are familiar with them. There is no difference to the applicability of policies if the equipment is being used outside of any Barlows UK Ltd premises.

5.4 Backups

If file content is being changed and not transferred regularly to the Barlows UK Ltd network, you must take your own backups of data from your Laptops, Desktops, Removable Storage, Mobile Phones, Tablets, Offsite Storage & Personal Devices on a regular basis. It is your responsibility to take regular off-line backups to a suitable storage device. Backups must be encrypted, physically secured and stored within the EU. **Storing data outside the EU is a criminal offence.**

5.5 Reporting Security Incidents

All security incidents, including actual or potential un-authorised access to Barlows UK Ltd system information resources should be reported immediately to GDPR team.

5.6 User Awareness

Users shall be made aware of their responsibilities in the prevention of unauthorised access to Barlows UK Ltd system information resources including but not limited to:

- That no equipment is left logged in and unattended without protection of an activated password protected screen saver.
- The need to be aware of this policy and all its provisions.

5.7 Suppliers & Sub-Contractors

Suppliers and sub-contractors must comply with GDPR

6. Disciplinary Process

Barlows UK Ltd reserves the right to audit compliance with the policy from time to time. Any disciplinary action arising from a breach of this policy shall be taken into accordance with Barlows UK Ltd Rules and Disciplinary Code as amended from time to time. Disciplinary action may ultimately lead to dismissal.

7. Deviations from Policy

Unless specifically approved in written form, any deviation from this policy is strictly prohibited. Any deviation to or non-compliance with this policy shall be reported to the GDPR team.

8. Format/Media

8.1 Paper

Theft of data from written sources can be as equally damaging and litigious as theft from electronic sources. Therefore we need to treat written information sources with as much care as electronic ones. If written records cannot be avoided they must be securely stored and must be confidentially shredded at the end of use.

- All used paper documents/records must be placed in shredding bags.

- Printed/written documents/records must not be left unattended on desks and must not be disposed of in general waste.

8.2 Removable Storage

No information should be removed from Barlows UK Ltd controlled environment without authorisation. If authorisation is permitted all removable storage must be encrypted. Removable storage may include memory sticks, CD-ROMS, SD Card, portable hard drive, photocopies, hand written notes, smart phone and tablets.

8.3 Verbal

Confidential and sensitive information can be communicated verbally. Care must be taken not to divulge or reveal sensitive information.

8.4 Email

Emails are not encrypted, consider carefully if confidential personally identifiable information is required to be sent by email within Barlows UK Ltd. Personally identifiable information **must not** be sent outside of Barlows UK Ltd via email.

8.5 Offsite storage

GDPR data legislation states that information cannot be stored outside the EU.

Due to the lack of knowledge of the physical location of cloud servers/services it is Barlows UK Ltd policy that cloud storage is not used unless the location can be proven. Such services are :-

Dropbox
Icloud
Google Docs
We Transfer

8.6 Personal Devices

Personal devices should not be used to process information from Barlows UK Ltd. If they are to be used for business related items no confidential personally identifiable information is to be processed, from Barlows UK Ltd, any of its suppliers, employees and customers, for example by email or photograph. The device must be password protected with a strong secure password. Any information being sent should be carefully considered.

Personal computing devices must NEVER be physically connected to any Barlows UK Ltd network.

8.7 Third party messenger services

3rd party services such as but not limited to Whatsapp & Facebook Messenger must not be used to send confidential personally identifiable information such as employee and customer information as defined by GDPR.

8.8 Credit card details

Details must not be retained or stored.

8.9 Waste paper

All documents that contain any personal or confidential information must be placed in the shredding bags for confidential shredding. Under no circumstances are documents to be disposed of in the general waste.

8.10 Work related applications.

Software applications such as job deployment and vehicle tracking are only to be used for business related activities.

8.11 Vehicles

All vehicles are tracked by a 3rd party telematics company for the sole use of the business. Information is stored by the telematics company and any information gleaned from the system must not be disclosed to a 3rd party without permission from the company. The images stored from a vehicle CCTV unit are only stored locally on the device. If an incident had been initiated either by the unit itself or by user interaction this will be saved on company servers and become viewable by the Fleet Committee.

9. Edge Protection

Barlows UK Ltd use the services of a third party to make regular scans of our public-facing internet connections to ensure our attack surface is minimised. All public-facing equipment must meet the requirements of Payment Card Industry (PCI).

10.Updates

It is expected that all computing equipment has the latest updates. Any equipment which is no longer supported by the manufacturer or any software which is declared end of life by its developer should not be used.

11. Redundant items

Redundant mobile phones, tablets, computers or memory sticks must be returned to Barlows UK Ltd for secure disposal and redundant documents must be securely shredded.