Royal British Legion Industries Information Security Policy	Effective Date	21st July 2011
	Location	i:\Policies\IT
Policy Title	Version date	June 2021
Information Technology Policy	Authored by	Kate Porter

This policy exists to serve a number of purposes:

- To ensure that Royal British Legion Industries (RBLI) can undertake its main business efficiently and effectively.
- To ensure only authorised personnel have access to software and data on the RBLI computer systems.
- To ensure the continued smooth operation of the RBLI's IT infrastructure.

Every single one of us is responsible for the security of data, this includes but is not limited to data we hold on our Employees, Customers, Suppliers, Residents and Attendees on our Welfare to Work or Armed Forces Programmes.

As a company our IT systems provide a significant amount of security including Firewalls, Anti-Virus Software and Encryption of sensitive data, however these systems will only ever go part way towards protecting the data that we hold. Therefore, it is important that we ALL understand our responsibility towards data.

1. Security

Access to RBLI systems is controlled through passwords. Users must never document or divulge their password to another person. All passwords must contain at least eight characters and must conform to the minimum requirements set by RBLI for complexity and composition. Passwords will be changed every 60 days.

The HR department are responsible for informing Business Systems of an individual leaving RBLI. Divisional Managers or those managers responsible for specific systems should inform Business Systems of any changes to an individual's access permissions should they change roles within the company.

2. Software

All computer software acquired by RBLI must be purchased through the Business Systems Department. No user may purchase software and the purchase of software by any other means such as credit cards, expense accounts or petty cash is expressly forbidden.

Anyone wishing to purchase software must first discuss with their Line Manager and in turn the Head of Business Systems who will source prices and authorisation for the purchase.

The Business Systems Department are responsible for ordering, installing the software and ensuring that it runs correctly on the PC or laptop.

All licences and media for software must be kept within Business Systems.

3. Software/Hardware Disposal

The Disposal of Software/Hardware used by RBLI may only be carried out by the Business Systems Department. Once a computer is deemed ready for disposal all software will be removed, where the licence permits the software will be re-used or stored for future use (OEM software will be disposed of with the computer as these licences are non-transferable). All RBLI data will be removed and the hard disk will be securely destroyed by an external company and proof of destruction provided. The asset register will be updated and the certificate of disposal/destruction will be held on file.

4. Evaluation Software (Freeware & Shareware)

Shareware, Freeware & Public Domain software is bound by the same policies and procedures as all software. No user may install any free or evaluation software onto RBLI systems.

5. Games & Screensavers

RBLI will not tolerate the use of any games or screensavers other than the standard windows screensavers, or the games which form part of your operating system. All screensavers will be set to enable after 5 minutes of inactivity and will be password protected.

6. Internet Downloads

No software, whatsoever, may be downloaded from the Internet without the permission of a Divisional Director and the Head of Business Systems. Access to the internet is provided for professional purposes only. Accessing inappropriate material is a disciplinary offence. Downloading and distributing inappropriate material is also a disciplinary offence.

The company reserves the right to monitor internet access, email traffic and Teams content on a site wide or random basis. This includes private e-mails where reasonable and proportionate to do so. Furthermore, the use of software filters will be used to prevent access to Internet sites deemed inappropriate to the Company's business.

7. Email Attachments

Users may not load or use any software received via e-mail. If you receive any files, which are not standard business documents, inform the Business Systems Department immediately.

8. Auditing

All users must be aware that RBLI periodically audits all computers. Sample random audits will be carried out and users will not be notified in advance that this will happen. Home areas on the network will also be audited.

9. Use of Personal Equipment

The use of non RBLI owned equipment such as PC's, Laptops, Smart phones, mp3 players, iPods, USB sticks, CD's, DVD's. Memory cards etc. can raise issues surrounding compliance, security, and data protection. You are not allowed to connect any equipment/device that is not owned by RBLI to any equipment that is owned by RBLI, including but not restricted to Company wireless networks.

10. Backup and Maintenance

All RBLI business data is replicated every 15 minutes for Disaster Recovery purposes and regular backups taken. This is stored on a secure staging server ready for restoring should the need arise.

11. Disaster Recovery

RBLI has a Business Continuity Plan in place and this is held as a separate document and is the responsibility of the Senior Executive Team. All RBLI business data is replicated every 15 minutes for Disaster Recovery purposes and separate regular backups taken on to a staging server.

12. Anti-Virus

RBLI uses Anti-Virus software to safeguard its systems from malicious code. This must not be removed or replaced with other vendor software. Currently we use Sophos which may update definition files several times a day, if you think that your anti-virus software is out of date please contact the Business Systems department immediately.

13. Data Protection

All computer processing of data relating to living individuals must be registered and be undertaken in accordance with the RBLI'S Data Protection registration. Such processing may only be made on computers owned by the RBLI and located within the premises of the RBLI.

Our systems enable us to monitor telephone, email, voicemail, internet and other communications. In order to carry out our legal obligations as an employer (such as ensuring compliance with our IT related policies), and for other business reasons, we may monitor use of systems including the telephone and computer systems, and any personal use of them, by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

The Do's and Don'ts When Handling Data

- Do not write down any passwords
- Do not disclose your password to anyone
- Do not leave your PC or laptop unlocked if you leave your desk
- If you print something, check you are sending to the correct printer and collect it immediately; do not leave it on the printer where someone else could see it.
- Do not allow non RBLI personnel to use company equipment or to look over your shoulder while you are working
- Do not log on and then let other RBLI staff use your laptop or PC
- RBLI operates a clear desk policy, do not leave anything with confidential data on your desk when you are not there
- Everyone should know the location of our Security Policies, if not then ask someone
- Report any security incidents immediately to your Line Manager no matter how minor they appear
- Do not leave mobile phones unlocked when not in use
- Clear down whiteboards etc. after use
- Delete Voicemails if you no longer need them
- If you do not recognise someone in your working area, challenge them, ask them who they are and report if necessary. Visitors should be wearing a visitors badge and should be escorted.
- Be aware of GDPR legislation and refer to RBLI training presentation if you need to, this is issued annually and all employees are expected to comply with this.
- Treat personal information as if it belongs to you or your family

14. Unauthorised Access/Hacking

Unauthorised access, or hacking, is an offence under the Computer Misuse Act. If any user believes they have access to unauthorised systems, software or data this should be reported to the Business Systems department immediately.

15. Access to Buildings and Offices

Access to RBLI premises is restricted to staff and authorised visitors only. All visitors must sign in at the location they are visiting and in general, should be accompanied around site or escorted to the location they are visiting. All staff are encouraged to challenge anyone they do not recognise. Access to restricted areas such as the server rooms should be closely controlled.

16. Email & Teams

E-mail is a very formal means of communication, treat e-mail as though you were engaged in written or verbal communication. Do not make defamatory, racial or sexual remarks about any person or organisation. E-mails can be used as evidence in a court of law. Do not use e-mails for confidential information, e-mail is not a secure means of communication. E-mail must not be used to send or receive pornographic material. E-mail is immediate; please remember this when constructing your e-mails. Offers and contracts made by e-mail are considered as legally binding. Jokes and sarcasm can be easily misinterpreted when using e-mail. Be very careful about the tone of e-mails.

Teams is a less formal means of communicating than email, but the same care should still be taken when using it as you would when writing an email and follow the rules in the above paragraph in the same way.

17. House Keeping

Each individual is responsible for housekeeping in their individual home areas and their email. Any unnecessary files or emails should be deleted to conserve space on the network.

18. Care of RBLI Equipment

IT equipment issued to anyone remains the property of RBLI. Equipment must be kept clean and no stickers or covers that would be difficult to remove should be attached to anything. If you are returning kit to RBLI please ensure it is cleaned before handing back.

19. Business Systems Help Desk

All support requests should be sent to support@rbli.co.uk, however if you are in urgent need of assistance, e.g. you cannot login or you think you have a virus on your computer, please call us.

21. Review of Policy

This policy will be reviewed on a regular basis and amendments communicated out to all users.

DISCIPLINARY PROCEDURES FOR BREACH

RBLI policies are implemented to safeguard RBLI from the many varying laws surrounding GDPR, data protection and information security. Any user found to be breaking these policies may be subject to disciplinary procedures.

Imagine how you would feel if your bank or your doctor lost your data and it was out there for someone to find, this is how you must think about the data that we handle. Losing or having someone's personal information stolen could result in Identity Theft and have an untold effect on the individual's wellbeing.

If RBLI has a security breach and is found to have not taken the necessary precautions to protect the data, we hold then there is the possibility of major fines or even prison sentences being handed out.

Failure to comply with the above points may results in access to systems being withdrawn or in disciplinary action