1. Introduction

Information and Communications Technology is an increasingly integral part of Balloo Hire Centre Ltd (Balloo) business operations, and it is standard for employees to use multiple technology devices (PCs, Laptops, tablets, Mobile phones and others) as part of completing day to day activities.

It is important that Balloo, as a business, uses technology in a manner that portrays the professionalism of the company. This policy has been drafted to guide all employees on acceptable use when using Balloo's systems (hardware and software) and the responsibilities and expected behaviours when interacting on any non-Balloo systems, e.g.: Social Media sites.

The objective of the policy is to ensure that Balloo IT hardware, software, mobile phones, data and information are protected from all threats, whether internal or external, deliberate or accidental. It is important to ensure Balloo employees, suppliers and customers are also protected from such threats. Balloo does not operate a BYOD policy (Bring your own device) Use of personal devices is not permitted.

It is the Policy of Balloo to ensure:

- Information is protected from unauthorised access.
- Valuable or sensitive information is protected from unauthorised disclosure.
- All software copyrights are respected and all terms & conditions of any license to which Balloo are a party are adhered to.
- The accuracy and completeness of information by preventing unauthorised modification.
  Individual accountability is established for appropriate system usage.
  Individual accountability is established for the security and maintenance of all IT hardware.

- Regulatory and legislate requirements are met.
- Balloo facilities and assets are only used for authorised activities.
- Balloo assets remain the property of the company.

At the core of the policy is the principle of individual responsibility for technology which Balloo provides to an employee. It is the employee's responsibility to ensure that this policy is adopted and followed.

Any updates on the guidelines to systems usage will be updated and new guidance issued.

2. Internet Use

If you have access to the Internet this is to be used in a manner which is consistent with and appropriate to professional business conduct. The Internet must only be used for authorised actives. When on the Internet, employees must regard themselves as representing Balloo and must conduct themselves to avoid bringing the Company into disrepute. Whilst primarily for business use, limited personal use is permitted before or after work hours and during lunch time; personal use should be reasonable and must not expose the Company to risk or adverse publicity as a result of misuse.

Any personal use of the Internet must not affect your ability to carry out your work. Please see below further guidelines regarding internet usage in the workplace:

- Maintain the security of your log-on ID and passwords at all times
- Do not change the Internet software configuration on your workstation.
- Do not download or install unauthorised software. If you require added functionality for your business, you should contact and request it from your depot manager. This is valid for all types of software, updates, patches, drivers etc.
- Refrain from sending confidential or private information via Internet mail (e.g.: Gmail or Hotmail accounts) unless authorised to do so.

- Downloading files must only be done from secure sites and only for Balloo purposes. Employees are not authorised to download games, music (incl. MP3), video sequences, screen savers; the download of files making Balloo liable for costs and licensing is not permitted.
- Do not transmit copyright protected material as this may contravene relevant and applicable laws. Employees are not permitted to store copyrighted material on company systems, including but not restricted to, MP3s and videos.
- Do not access, publish or transmit material of a potentially offensive or illegal nature. Use of internet services via the IT Infrastructure for illegal or unlawful purposes, including copyright, infringement, obscenity, libel,slander, fraud, defamation,plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes and computer tampering is prohibited. Especially all kinds of pornography
- Report any incorrect, inflammatory or misleading portrayal of Balloo on the internet to your manager.
- Employees are not permitted to use unauthorised internet-telephony services (e.g.: personal Skype calls).

3. Email Use

Balloo seeks to promote and make proper use of technology in the interest of its business and its employees. Email is a key business tool and is provided primarily for business use.

- Balloo recognises that employees may need to use email occasionally for personal purposes, which should not interfere with you work.
- Please note email phishing scams are on the rise if you believe you have received a phishing email DO NOT click on any attachments or links. Delete the email and inform your line manager.

We use Microsoft Outlook as our email platform, and you will be required to enter a complex password containing letters, numbers and symbols. This password will change monthly.

Please ensure this password is not written or shared with anyone internal or external to the organisation. If you believe your password may have been compromised, please contact your line manager immediately.

This section outlines the responsibilities of employees using Balloo email.

Emails should be drafted with care. Due to the informal nature of email, it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from your computer

You should not send unnecessary emails or copy others into the message without good reason. Unnecessary emails wastes company memory and congests the email system.

Emails of a personal nature both sent and received are to be kept to a minimum during working hours.

You must not use emails to send or forward any materials that might cause offence to any person communicating with anyone via email you should not make or forward any statement which could be construed as;

- Defamatory;
- Sexist or racist in nature;
- A derogatory remark relating to a person's sex, race, disability, sexual orientation, gender reassignment, religion, belief, political beliefs, age, ethnic origin, colour or nationality (this list is not exhaustive);
- For criminal purposes; or
- Being of an offensive or obscene nature

You must not send chain letters via email, if you receive virus warnings or chain letters via email, or receive anything that is questionable or illegal, contact your Line Manager.

You should regularly review and manage/delete e-mails to prevent over-burdening the system. Please note, the 'All Users' address facility is not to be used for messages of a personal nature.

- Periodically IT will review the size of individual email accounts and provide guidance to any users not using or managing their email accounts effectively.
  There is a 10Mb file size limit for sending emails both externally and internally.
- It is important to note that sending confidential business information via personal Internet mail messaging Apps (e.g.: Gmail, Hotmail, Whatsapp, Messenger) unless authorised is prohibited.
- Please ensure you follow the guidelines set for your email signature (this can be obtained from the Marketing Department. This is to ensure consistency of the Balloo branding.

4. Mobile Phones and Mobile Devices

Mobile phones and other mobile devices are essential tools for Balloo. The misuse of these tools can lead to unnecessary running costs and is a waste of valuable resources.

. 5 Company Phones

Balloo will provide eligible employees with Company Mobile Phones and/or other Mobile Devices for the sole purpose of conducting Company Business. It is the responsibility of the employee to ensure their Company Mobile Phone and all other Devices are kept charged and in their possession during working hours.

Employees are not permitted to use or send MMS (picture) messages or make video calls from any Company Device without the authorisation of their Line Manager. Furthermore, employees are not permitted to make calls/texts to premium rate numbers without the authorisation of their Line Manager.

Sensitive personal information, as defined by the General Data Protection Regulations 2018 (GDPR), should not be stored on a mobile device (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life and criminal convictions).

Use of the SMS facility should be kept to a minimum and should be for business purposes only.

6. Personal usage of Company Phones

- Personal calls should be kept to a minimum and should not in any way interfere with your work.
- Personal SMS messages should not be used unless in exceptional or urgent circumstances.
- Employees are authorised to send/receive Data messages for Business purposes but must remain within the limits of the agreed data bundle.
- The Company will not be liable for any Benefit in Kind implications (such as taxation) which result from Personal use of a Company Mobile Phone or Device.

7. Data Usage

Data usage on all Company Mobile Phones and Devices must be compliant with the data limits set in the agreed tariffs and also the ‘internet use’ and ‘email use’ sections of this policy.

8. Data Tethering

Tethering is a technique in which a Mobile Phone is used as a wireless access point to the internet for another Mobile Device (e.g. Laptop/Tablet Computer). Tethering is permitted on any Company Mobile Phone or Device providing there is a good business reason. Employees who are found to have incurred significant costs as a result of tethering any Devices together without good business reason, may be liable for reimbursing the cost to the Company. Any concerns which arise due to tethering costs will be investigated with the Employee and their Line Manager.

9. Expenses

The Company monitors Mobile/Device usage and excessive use may result in the privilege being removed. The Company reserves the right to seek re-imbursement of cost which is deemed excessive and make the appropriate deductions from Payroll for amounts in excess of the agreed limits.

10. Foreign Use

Your phone is intended to be used primarily within the UK for Business Use. It is not intended to be taken abroad as standard. If you are planning on taking your phone abroad you must complete the following steps:

- Agree that it is acceptable with your line manager
  Keep call and data use to a minimum.
- Inform your Line Manager at least 2 weeks (or as early as you can) prior to your departure so we can contact our current provider to try and amend the contract to reflect usage abroad.
- Turn off data roaming (only use this if no other alternatives apply).
- Look to utilise free Wi-Fi hotspots where possible if you need to download significant data files.
- You remain responsible for appropriate use of the phone when abroad. Excessive charges will be recharged.

11. Miscellaneous

Any loss or theft of any Company Mobile Phone or Device must immediately be reported to the Police. Any subsequent Police reference numbers or information must then be promptly provided to the IT team. Users must take appropriate measures to protect against the accidental loss, damage or theft of Balloo information held on mobile devices, especially if that information relates to personal data.

- Do not allow unauthorised individuals to use your Mobile Phone or Device.
- You must return all Company Mobile Phones and Devices and any additional equipment to your line Manager on or prior to the last day of your employment with the Company, including any PIN number.
  It is essential that we as a business are seen at all times to be using every available technology asset in a manner that portrays the professionalism of the Company.
- Failure to comply with the guidelines on mobile phone usage may result in disciplinary action or for Balloo to seek reimbursement costs.
- For further information regarding Mobile phones/device usage please contact your line manager.

12. Smart Phone Usage Policy

Smart phones will be left relatively ‘open’ from a usage perspective. This is to allow you to customise to your business requirements.

The following provides a summary of the guidelines / principles for using the phone. Failure to adhere to this guidance may result in the phone being locked down. **Please note, in the event of excessive costs being incurred you will be recharged the cost.**

13. Initial Instructions

- Devices must be configured with a secure Pin which will be provided to you on handover of the device.
- Devices should not be connected directly to the Balloo internal corporate network
  (Balloo Employee WiFi or Guest WiFi).
  Wherever possible you should look to connect via a Wi-Fi connection rather than a 3G/4G connection.
- Free Wi-Fi connections are available in numerous locations and you should seek to connect to these wherever possible.Please ensure the network is trusted before connecting WiFi.
  This approach will help reduce any risks associated with exceeding your data limit.

14. Personal Smart Phone Responsibility

- The phone and all charges incurred on it are your personal responsibility. You should monitor both call and data charges on a regular basis to ensure you do not exceed expected limits.
- The phone has been set up in line with agreed Balloo controls and requirements. The standard phone configuration should not be edited or changed by the user. Such a change will be considered a breach of policy and the phone may be withdrawn. If you have any major issues with the phone requiring such action contact your line manager.
- Balloo retains the right to monitor usage and remove any applications deemed inappropriate for work duties. We have not applied many restrictions to the phone and we expect this to be respected. Any misuse of this may be investigated accordingly.

15. Data Limit

Smart phones are given a monthly data limit. Following a number of tests, this limit should be more than required for general business use. If you exceed this limit Balloo will incur additional costs which may be subsequently recharged to you if this usages was incurred as a result of poor practice or non-business use.

16. Downloading Apps

- The phone has been setup with access to the Google Play Store. As such you are able to download Apps to your phone. We have allowed this policy to provide you with flexibility to manage your own business App requirements. You should not download any Apps which are not appropriate (e.g.: social media, high data usage apps) and all Apps charges are your personal responsibility.
- Applications must only be installed from approved sources such as the Windows App store. Installation of Apps from un-trusted sources is forbidden.
- We recommend that you do not download any Apps which you must pay for because in the event of any problems with your phone IT may need to delete the Apps and these may not be recoverable.
- Balloo will not be liable for the cost of these Apps either during employment or in the event of leaving Balloo.
- Apps should be downloaded when on a Wi-Fi connection as this will reduce mobile data usage.
- Any Apps considered inappropriate or result in high data usage may subsequently be deleted from your phone. Balloo will not be liable for the cost of these Apps.

17 . Additional Information

Users must report all lost or stolen devices to your Line Manager immediately.
If a user suspects unauthorised access to company data via a mobile device, they must report the incident to Line Manager.

- Users should only load work data essential to their job onto their mobile device(s).
- Devices must not be jailbroken/unlocked or rooted or have any software/firmware installed designed to gain access to prohibited applications.Users must not load pirated software or illegal content onto their devices.
- Devices must be kept up to date with manufacturer or network provided patches. App and device updates should only be installed over WiFi.
- Users must not merge personal and work email accounts on their devices. They must only send company data through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Line Manager.
- Users must not use corporate work stations to back up or synchronise device content such as media files, unless such content is required for legitimate business purpose.

18. Personal Responsibility

Balloo provides many different IT assets to its employees to support day to day business operations. Although not an exhaustive list these IT assets include such devices as mobile phones, laptops, notebooks, Smart Phone, 3G air cards and memory sticks.

It is the responsibility of the individual using the asset to ensure it is used in an appropriate way. Please see below guidelines associated with this:

- The employee must follow any specific guidelines and training associated with the IT asset's use.
- Do not leave the asset unattended at any time. Where this is unavoidable, it should be locked away in either the back of the employee's Company van or the boot of their Company car.
- Any loss of the of the asset must be reported to the police and your line manager with any police reference number(s) to be provided.
- Users must take appropriate measures to protect against the accidental loss, damage or theft of Balloo IT assets and the data held on IT assets, especially if it is personal information.
- IT assets (mobile phones, laptops, notebooks etc.) should be stored within the Employee's home address/place of residence overnight.
- Under no circumstances should IT assets be left visible in vehicles overnight.
- IT assets should not be stored in insecure places such as under a passenger seat/in glove boxes etc.

If you are uncertain, or in any doubt, about the appropriate measures to protect assets and information, contact your line manager.

Balloo reserves the right to charge the employee for the replacement cost (based on purchasing a new asset) for any IT asset where it believes the above guidance has not been followed.

19. Security and Identity Theft

Social networking websites are a public forum and as such employees should not assume that their entries on any website will remain private.

Balloo employees must be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out.

Social networking websites allow people to post detailed personal information such as date of birth, place of birth, favourite football team or school information which can form the basis of security questions and passwords. Employees should:

- Ensure that no information is made available that could provide a person with unauthorised access to Balloo and/or any confidential information.
- Refrain from recording any confidential information regarding Balloo on any social networking website.

20. Disciplinary Action

Employees are responsible for complying with this Policy at all times. Breach of this policy may result in their mobile phone/device or IT asset privileges being suspended or permanently revoked.If appropriate, disciplinary ac on may be taken in accordance with the Balloo disciplinary policy.

For further information regarding the Balloo system usage please contact your Line Manager.

21. Monitoring

The Company reserves the absolute right to monitor employees' use of e-mail
The Company reserves the absolute right to monitor employees' use of the Internet.

22. User Manual

You must familiarise yourself with and follow the operating procedures laid down in the User Manual.

Mark Grundy
General Manager

Reviewed Feb 2022