SHIP TO SHORE
ALWAYS SECURE

Carnival UK
Box Acceptable Use Terms

Security Compliance & Risk

Carnival UK Security Policy
[May 2020 v1.0]

1.1. Protecting our information

As employees of Carnival UK we're all required to understand the risks associated with handling our data inside and outside the business. These risks are not always obvious so we have security controls in place to help protect us all.

The laws and regulations around information are also constantly changing so these terms of usage have been written to outline key accountabilities and working practices whist sharing information via the Box cloud platform. To ensure we protect our information, everybody must work within these guidelines to protect the security and privacy of ourselves, our colleagues and our guests.

1.2. Contacts and Further Information

For further information regarding the information security policies, standards and guidelines listed within this document please refer to the Carnival UK IT policies page on the bridge or contact IT Security/ITD/CarnivalUK

The **Data Governance** and **Privacy teams** can provide further advice on the proper use and classification of guest data, and if the sharing of that data to certain suppliers or end users is appropriate for the business. If you're unsure or have new requirements for sharing guest data outside of Carnival UK, please contact those teams for guidance.

1.3. The Box Service

Box is Carnival UK's approved cloud platform for file sharing and collaboration, other similar tools not approved for use when sharing CUK information, however you may use approved services when receiving files from trusted business sources eg. Other Carnival Brands. The purpose of the platform is provide accessible ways to share information and work with others in a secure way.

The Box platform is not intended to replace existing on premise file storage such as our share drives. As such, Box should not be used as the sole or permanent storage for your data and will be subject to time limited retention periods to ensure data is not stored longer than is appropriate.

1.1. Data Classification and Protection

It is Carnival policy that we classify our information to indicate the need, priorities and expected degree of protection when handling data. These protections are in place to safeguard us and our guests and are particularly important when we share information outside of the organisation.

All information stored on Box must be classified as per the table below, more information on data classification can be found in the Carnival Data Classification Policies and standards.

CLASSIFICATION:	BRIEF DESCRIPTION	EXAMPLES
HIGHLY SENSITIVE	This is non-public or regulated business information that required handling precautions.	• Pre-release financial results • Corporate level strategic plans • Personal financial or credit card information • Biometric information, such as fingerprint or retina data.
CONFIDENTIAL	This is non-public information that is proprietary, private, sensitive, or subject to contractual or other legal obligations of confidentiality. This data must only be made available to individuals with a business need and a right to know.	• Business plans • System specifications • Unreleased ship designs • Personnel records • Internal audit reports
INTERNAL USE ONLY	Generally available to employees and approved non-employees. It should be limited to use within Carnival and its partners on a need to know basis.	• Internal project reports • Training manuals and materials • Organizational objectives • Carnival or Brand newsletters • Organization charts • Procedure manuals
PUBLIC	Once public information has been approved for release, there are no unauthorized disclosures. Copyright or trademark protections may apply	• Marketing or advertising literature once it is issued • General product information • Job openings Announcements

For more guidance on how to classify information when using Box please refer the Box User Guide

1.2. Data Classification Protection Summary

Our responsibilities when protecting our information changes depending on the classification. The below matrix provides a summary of the key owner and user requirements that must you must apply before we share information on any platform including the Box

	CLASSIFICATION			
Control	**Public**	**Internal**	**Confidential**	**Highly Sensitive**
Document Labelling	None	Label as 'Internal'	Label as 'Confidential'	Label as 'Highly Sensitve'
Access / Sharing	Anyone	Internal & authorised external parties	Authorised internal & external parties only	Authorised internal & external parties only (strictly need to know) **PLUS** For access to Protected Health Information & Electronic Protected Health Information, a Business Associate Agreement is required for all external entities & representatives
3rd Party Conditions	None	May be subject to NDA	Subject to NDA & contractually obliged to secure our data	Subject to NDA & contractually obliged to secure our data

For more guidance on the requirements to protect our information please refer to the Carnival Data Classification Policy and Standard.

1.3. Accountabilities

Box is a versatile file sharing and collaboration tool however accountabilities related to sharing our information must be understood and exercised whilst using box to ensure we follow secure practices.

Information Owners (Owners): are the managers of organisational units (typically VP level) that have primary accountability for the information assets (data) within their authority

- Owners are accountable for defining their own operational process and procedures for authorising the access and sharing of information within their organisation
- Owners are responsible for ensuring authorisation for the sharing of information with external parties are documented (including what was authorised, by who and with whom)
- Owners are responsible for ensuring information under their control is classified and labelled correctly when it is created
- The Owner is responsible for defining processes and procedures that are consistent with these terms and our Global Data Classification Policy & Standard

Information Users (Users) are the individuals, groups, or organizations authorized by the Owner to access and share information.

- Users must confirm authorisation from the **Owner** (or approved delegate) before sharing Confidential & Highly Sensitive information with other Carnival employees
- Users must request authorisation from the **Owner** (or approved delegate) before sharing any non-public information with external parties
- Users are responsible for ensuring the information stored and shared on Box is classified and handled appropriately and in line with the owner's classification
- Users must maintain the security of information accessed, consistent with the **Owner's** approved safeguards while under the User's control
- Users are responsible for confirming the appropriate non-disclosure agreements and contractual obligations are in place with external parties before sharing information.
- Users must physically safeguard devices which house corporate and personal information such as company provided mobile phones, laptops and tablets
- Users are responsible for familiarizing and complying with our Data Classification and Handling Policy and Standards when sharing information

1.4. Third Parties

The following are key terms and conditions apply to all external/third parties (i.e. outside of Carnival UK or Carnival Operating Companies) when accessing Carnival UK information via the Box. For further information on third party security standards please refer to our global IT security policies and standards.

- **Third parties** must access Carnival UK information on Box via a Box Account
- **Third parties** can use Box to share data with Carnival, but users must be careful downloading any suspicious content.
- **Third parties** must apply rigorous security controls (compliant with Carnival UK information security standards) when handing Carnival UK information
- **The Owner** is **accountable** for ensuring third parties accessing our information have the appropriate non-disclosure agreements in place with Carnival UK
- **Users** are **responsible** for confirming the appropriate non-disclosure agreements and contractual obligations are in place with external parties before sharing information
- **Users** should continue to use existing secure mechanisms (i.e. SFTP / APIs) already set up with third parties to transfer information
- **Users** are responsible for managing appropriate access and permissions for information and folders that have been shared with third parties.
- **Users** must regularly review third party access and permissions for information they have shared and remove access where it is no longer required
- **Users** are responsible for making external parties aware of our applicable terms & security standards before sharing Carnival UK information

1.5. Regulatory Compliance

As part of specialist core activities or processes you may be involved in through your job, you must ensure that you follow the relevant legalisation when sharing our information including:

- Financial Information – Sarbanes Oxley (SOX)
- Payment card information – PCI DSS (Payment Card Information Data Security Standard)
- Personal Information – GDPR (General Data Protection Regulations)
- International Maritime Organisation (IMO and HESS)

If you are involved in handling these specialist types of information, you will be required to understand how the requirements relate to sharing that information and following the Carnival UK processes that are in place.

1.6. Box account approval and sharing externally

Box accounts will need to be requested by the user and authorised by their respective information owners via service request (SR). In order for the request to be processed and the account set up the owner (typically VP) will need to authorise the request for the account and any intent to share information with external parties. Sharing with external parties is enabled in Box via a 'white list' of trusted partners which is updated via user request and appropriate approval.

The purpose of the SR process is to provide the opportunity for owner's to review an individual's request to use Box to share information before being granted access. The SR process does not replace the need for internal processes to approve the sharing of information on Box. Owners must ensure the internal processes are in place to maintain appropriate visibility and authorisation for sharing information under their control.

1.7. Leavers Process

On exiting the business it is the responsibility of the individual's line manager to ensure the users account has been disabled and any data to be retained repatriated to permanent Carnival UK file storage.

1.8. Corporate and Personally Owned Devices

The use of mobile devices (corporate or personal) introduce risks to our information. Mobile devices are at a higher risk of being lost, stolen or compromised. In addition **personal devices** (i.e. devices not provided and managed by CUK) are outside of our technical control and do not always meet the security requirements necessary to keep us and our guest's information safe.

Box works on most devices however the access and storage of sensitive company information is restricted to **Carnival UK owned devices** and is prohibited on **personally owned devices**. As such the **download** of '*confidential*' and '*highly sensitive information'* on **ALL** smart devices (i.e. corporate and personal phones and tablets) is disabled within Box.

However If there is a business critical need to use Box on personally owned devices to access less sensitive information this will require user acceptance of the **Personal Device Activation Agreement** (PDAA) terms detailed below and authorisation from your leadership team via the Box Account SR process.

1.9. Personal Device Activation Agreement

By accepting the below terms you agree to own the risks associated with protecting Carnival UK information and be bound by the conditions laid out.

- All mobile devices must enforce a password/PIN
- Device encryption must be enabled to protect data at rest. This includes encryption of removable memory cards where applicable.
- The ability to remotely wipe a device must be enabled.
- Jailbroken or Rooted devices are prohibited
- Storage of credit card, public health information, guest(s) information on personally own mobile devices is prohibited.
- All Carnival UK data transmitted to/ from and stored on personal devices is owned by and is the exclusive property of Carnival UK. Treatment and responsibility of Carnival UK information on the mobile device falls under the Carnival UK Data Protection and Privacy Policies and the Carnival UK IT User Policy.
- Carnival UK has the right to remotely manage and administer the personal devices that connect to the Carnival UK network. This includes the right to impose security policies which include, but are not limited, to setting a device password (PIN), setting an inactivity timeout, hardware encryption, and wiping the device.
- The employee must immediately contact the Carnival UK IT Service Desk at 44 (2380) 65-6000 if their mobile device is lost or stolen in order to have all information on the device erased and disabled. The employee may not sell or trade-in their device without notifying Carnival UK and getting a positive verification that the device has been erased and de-authorised from Carnival UK services.
- When access is no longer authorised, Carnival UK has the right to erase all information on the employee's personal mobile device. Carnival UK is not responsible for backing-up or restoring any personal information stored on the device. The employee is responsible for backing up and restoring personal information on the mobile device. Carnival UK discourages personal backup of company information. The employee must comply with all Carnival UK Data Protection and Privacy Policies and the Carnival UK IT User Policy in respect of any Carnival UK information that is backed up from the device to a system outside of Carnival UK control. Carnival UK may, at its discretion, demand inspection of the employee's backups and require proof of deletion of company information. Employees will remain liable without an expiration date for leaked information that is traced in the future to copies of their making.
- IT Support Desk will not support issues related to the personal devices' Operating System.
- IT Support Desk will not support wireless configuration and settings related to the wireless carrier.
- IT Support Desk will not support hardware related issues with the personal device.
- IT Support Desk will not support third party applications on the personal device.