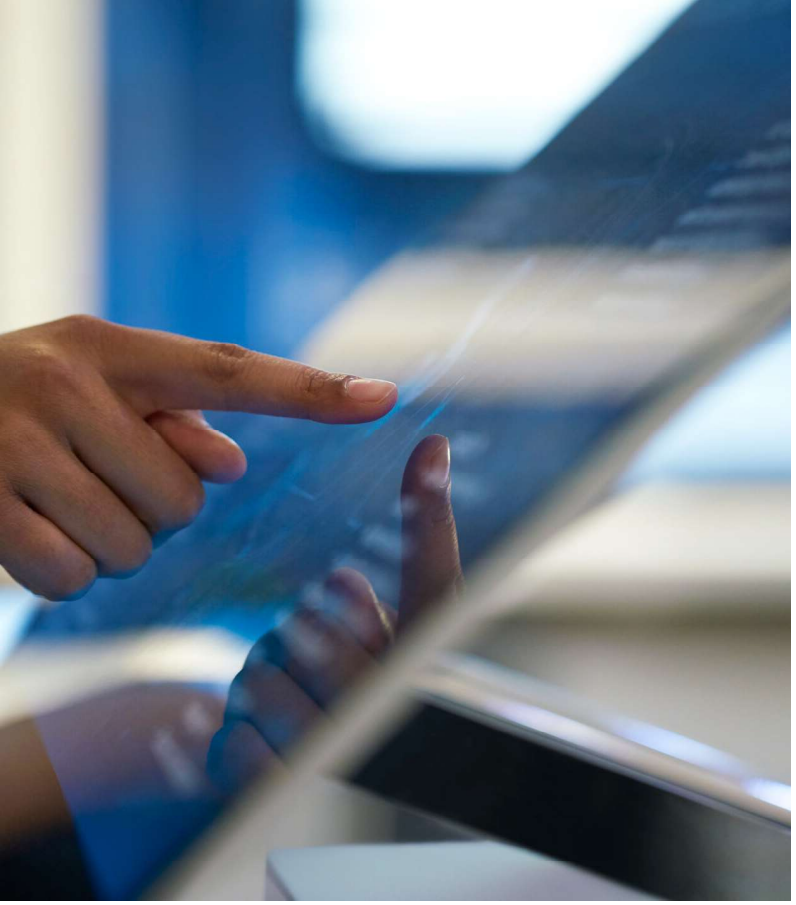

Third Party IT Acceptable Use Policy

Your Responsibilities

Safeguarding our resources

Rolls-Royce technologies, intellectual property ("IP"), and commercially sensitive and confidential information are vital assets of our business. We must protect them from unauthorised access, use and disclosure.

Our Company Information Systems are fundamental to our business operations and processes. We are committed to protecting our systems and maintaining compliance to legal, regulatory and contractual requirements. All users of our Company Information Systems must therefore follow policies and processes applying to our Company Information Systems and must not bypass or attempt to bypass any technical or security controls. Users are only provided access to and should only access Company Information Systems for the purposes of performing their role.

You are responsible for the safe and secure use of our Company Information Systems and the protection of data, and this document sets out your responsibilities and the behaviours we expect from users.

Glossary

Company Information System means a discrete set of information resources organised expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including, specialised systems, for example: industrial/process control systems, cyber-physical systems, embedded systems, and devices.

System(s) means all types of computing platforms that can process, store, or transmit Rolls-Royce data.

Your Responsibilities

- You will not access or use our Company Systems:
  - in a way prohibited by law, regulation, governmental order, or decree;
  - to violate the rights of others;
  - to spam or distribute malware; or
  - to try or to gain unauthorised access to or disrupt any device, account, network, or service.
- You must only use our Company Information Systems and data to deliver our business activities, processes, and services.
- You will always act in an ethical manner when using Company Information Systems, including online and social media platforms.
- You must not seek any access permissions and privileges that are not required to perform your role.
- You must not use Company Information Systems to access, copy, store or transmit anything considered to be offensive, obscene, or inappropriate, or that which we do not have permission or authority to engage in.
- You will only use our resources for authorised business purposes, and for delivery of your contracted service role.
- You will avoid waste and protect our Company Information Systems and data from theft or damage.
- You will not bypass, alter or ignore protective IT security controls or physical security systems which includes (amongst other actions) changing or attempting to change the configuration of any of our devices, systems or software, unless you have been authorised by us to do so or installing software or connecting devices or systems to external networks without our authorisation.
- You will ensure you log off and complete all shutdown processes at the end of your working day.
- You will reboot your computer at regular intervals to ensure required operating system and software updates are installed.
- You will seek prior written approval before travelling overseas and accessing Company Information Systems or storing our data on removable media.
- You will handle our information in accordance with its classification, and ensure all documents created are marked appropriately and in accordance with the Rolls-Royce Data Classification Guidelines.
- You will take care when opening emails from unknown or unexpected senders and be cautious when clicking on links or opening attachments.
- You will not browse, post, or interact with websites likely to be deemed unacceptable with our policies, even if they are not blocked from access.

IT Account

Company Information Systems contain sensitive and confidential information, so access is permitted to authorised people only.

When your application for an IT account is complete you will receive a username and temporary password to access Company Information Systems. On first access you must change the temporary password by following the instructions for password requirements provided to you.

You must not:

- share your user ID and/or password, or any Group ID, with anyone;
- share your device hard disk encryption key with anyone;
- write down your passwords (any storage of passwords must be via a password manager approved by us);
- leave your computer or session unattended and logged in at any time, ensuring your session is locked and/or device is securely locked away before leaving it unattended; and/or
- ignore any requests to change your passwords (following the instructions provided to you).

If you are issued a remote access account and key fob/token with password, you must keep them safe. If you lose your key fob/token, please inform the IT Service Desk as soon as possible.

Monitoring and Consequences of Breach

Your use and access to Company Information Systems is monitored as necessary to comply with legal and regulatory requirements and for legitimate business purposes (e.g., resolve technical issues, identify, and investigate misuse, assess policy compliance, etc.).

If you discover suspected or actual policy breaches or any security incident, you must send a report immediately to the Global Security Operations Centre (SOC).

Our Code and Group Policies

You must read Our Code and Group Policies to understand how you are expected to comply with, uphold your responsibilities for accessing and ecurely and safely using Company Information ystems, and the consequences for breaches. If you quire further guidance, please contact your Sponsor or Vendor Security Manager (VSM)