HOUSES OF PARLIAMENT
RESTORATION & RENEWAL

# Bring Your Own Device (BYOD) Policy

## R&R Data & Digital Service

# Table of Contents

# 1 Introduction

The purpose of this Policy is to protect the Restoration and Renewal Programme's (R&R) digital environment including the services and data held within it. It sets out the responsibilities of all those (here on known as the R&R Data and Digital Services "Customers") who use Bring Your Own Devices (BYOD) to connect and subscribe to R&R Digital Services.

# 2 Purpose

Data & Digital (D&D) Services recognise the benefits that can be achieved by allowing staff to use their own digital devices when working, whether at home, in the office or while travelling. Such devices include laptops, smart phones and tablets (see section 3 Scope), and the practice of using these devices for business purposes is commonly known as 'Bring Your Own Device' or BYOD.

If Customers wish to BYOD to access R&R Data & Digital Services, they may do so, provided that they follow the provisions of this and other associated R&R Data & Digital Service policies. The D&D Team will place as few technical and policy restrictions as possible on BYOD subject to appropriately protecting the confidentiality, integrity and accessibility of R&R Data & Digital Services.

The fulfilment of these responsibilities not only protects the data belonging to the Programme but also reduces the likelihood and impact of a cyber-attack, data breach or other illegal and damaging activity. The D&D Services teams will support all its Customers in this endeavour.

# 3 Scope

This Policy applies to Customers of the R&R Digital Service, whether permanent, temporary or guest. For the avoidance of doubt, this includes employees, agency/interim staff, third-party providers, sub-contractors and visitors or anyone else authorised to subscribe to R&R Digital Services. The Policy must be adhered to by all Customers and is for the protection of the R&R Digital environment and the data held within it

For the purposes of this policy, the following are considered BYOD:

- Smart and other types of mobile phone.
- Tablet computers.
- Laptop, notebook, netbook and Chromebook computers.
- Desktop computers.
- Personal Digital Assistants (PDAs).
- Any personally owned digital device capable of accessing R&R Data and Digital Services.

# 4 Exclusions

This Policy does not apply to devices provided by the R&R Digital Service Centre.

# 5 Definitions

| | |
|---|---|
| R&R Data & Digital Service | The environment and services offered, and the data held within, as supplied and supported by the D&D Team. This includes but is not limited to R&R networks (wired, wireless and remote connections to these networks), all D&D supplied equipment and applications, software and digital services provided via the Internet. The data concerns the data and information belonging to the R&R Programme. |
| R&R Data & Digital (D&D) Team | The dedicated R&R team that provides the R&R Digital Service. |
| R&R Digital Service Centre | A sub-team within the R&R D&D Team which is tasked with the overall day-to-day operational support of the R&R Digital Service. |
| Customer | A subscriber, internal or external, to the R&R Digital Service. |
| BYOD Device | Bring Your Own Device. Digital devices belonging to Customers (not owned or provided by the R&R Digital Service Centre) and used by them to access, view and modify R&R digital services and data, whether at an office or remotely (at home and / or while travelling). |

# 6 Responsibilities

## 6.1 Developing and Assuring the Policy

The D&D Team is responsible for maintaining and updating the BYOD Policy and will continually monitor usage of BYOD. Where necessary to protect the R&R Data & Digital Service, D&D may temporarily or permanently halt use of one or more types of BYOD. D&D may for the same reason also temporarily or permanently halt use for a specific Customer or Customers group of BYOD.

## 6.2 Data and Digital Customer Responsibilities

By using any part of the R&R Digital Service, Customers accept that they are individually accountable and responsible for the following:

- The purchase or procurement of any BYOD devices that they wish to use. Customers will not be reimbursed in full or part for the cost of these devices.
- Payment in full of all costs associated with data plans (home broadband, mobile SIM's etc). Customers will not be reimbursed for the cost of personal data plans used to access D&D Services.
- Payment in full of any manufacturer or 3rd party costs incurred by the Customer to support, maintain, repair or insure BYOD devices.
- Protection of the confidentiality, integrity and accessibility of all D&D Services that they have access to.
- To not attempt the removal, download or transfer of D&D data to non-D&D environments unless expressly given permission to do so by the Senior Information Risk Officer (SIRO).
- To abide at all time by the *R&R Acceptable Use of Digital Services Policy.*
- To abide by the *R&R Data and Digital Travel Policy* if a BYOD device has, prior to the effective date, been used in a Restricted Country (see policy for definition).
- To report any suspected cyber security incidents involving BYOD to the Digital Service Desk, and
- To report any breaches of the above Customer responsibilities and this policy to the Digital Service Desk.

# 7 Policy Musts and Must Nots

By using BYOD, the Customer agrees to abide by and uphold the following:

## 7.1 Musts

Customers must:

- Adhere to the authentication requirements stipulated by the R&R Digital Service Desk for each BYOD device type including setting up passwords, passcodes, passkeys or biometric equivalents to secure and prevent unauthorised access.
- Keep BYOD device Operating Systems up to date, particularly with regard security patches.
- Install and keep up to date anti-virus software where the BYOD enables such software to be used.
- Allow if requested, the R&R Digital Service Desk to install remote management software to enable BYOD devices to be wiped if lost or stolen.
- Ensure that all D&D documents are stored only in D&D approved OneDrive and SharePoint repositories.
- As soon as possible, report to the Digital Service Desk the loss or theft of any BYOD device that has been used to access D&D Services.
- As soon as possible report to the Digital Service Centre any malware, virus or ransomware infection of a BYOD device. Use of the BYOD and access to R&R Data and Digital Services should be ceased immediately.
- Assist and support the R&R Digital Service Centre in carrying out its legal and operational obligations should it be necessary to access or inspect D&D data stored on a BYOD.

## 7.2 Must Nots

Customers must not:

- Use BYOD devices for any purpose that contravenes UK criminal or civil law including the use of unlicensed software to access R&R Digital Data and Services.
- Store or hold R&R data or documents on BYOD device local disk or memory storage.
- Attempt to circumvent the device manufacturers in built security mechanisms in any way. E.g. Jailbreak.
- Lend, loan, transfer or sell BYOD devices to family, friends or any other person until access to R&R Data and Digital Services has been removed or disabled by the Digital Service Desk and the Customers D&D password changed.

# 8 Monitoring and Access

The Digital Service Centre will not routinely monitor BYOD devices. However, it does reserve the right to:

- Prevent access to D&D Services in order to manage or prevent breaches of R&R Security or Acceptable Use policies.
- Take all necessary and appropriate steps to retrieve and / or delete R&R data and documents downloaded to or stored on BYOD devices.
- Monitor and log data traffic transferred between BYOD devices and R&R Data and Digital Services.

# 9 Training Requirements

Customers will be given a copy of this Policy as part of their welcome email. It is the Customer's responsibility to read and understand the Policy.

Periodic training will be given to customers to enhance their understanding.

# 10 Monitoring and Compliance

Compliance with all responsibilities will be audited. This may be performed manually, through ad-hoc activities or via automated capture of data, e.g. completion of Cyber Security training, attempts to access restricted sites, etc.

Unintentional non-compliance will not normally require any action, except for further education of the Customer.

Intentional non-compliance is more serious and appropriate action will be taken on a case by case basis. Consequences of data and digital breach may include, but are not restricted to:

- escalation to the Customers line manager;
- possible restriction in accessing the R&R Digital Service; and/or
- disciplinary sanctions or action,

and in extreme cases:

- civil action against the Customer and/or their employer; and/or
- notification to the appropriate authorities that there has been a crime or regulatory infringement.

# 11 Associated Documentation

R&R Data & Digital Service Acceptable Use Policy

R&R Data and Digital Travel Policy

The Parliamentary Digital Service also has standards and policies relating to the use of their services and data. These should be referred to should a Customer require access to its service offerings. This is not connected to, and has no bearing on, the R&R standards and policies.

# 12 Equality Assessment

An Equality Assessment has been performed against this document and can be found in Equality Analysis_BYOD Policy available from R&R D&D Communications.

**Sarah Johnson**
CEO, Sponsor Body
September 2020

**David Goldstone**
CEO, Delivery Authority
September 2020