HOUSES OF PARLIAMENT
RESTORATION & RENEWAL

Acceptable Use of Digital Services Policy

R&R Digital Service

Table of Contents

1 Introduction

This Policy is a User Guide, intended to protect the Restoration and Renewal Programme's (R&R) digital environment including the services and data held within it. The provision of a network account to the R&R Digital Service implies that the person holding that account is a subscriber to the R&R Data and Digital Services. This Policy sets out the responsibilities of all those who connect and subscribe to this Digital Service, whether internal or external; from here on known as the Data and Digital (D&D) Services "Customers".

2 Purpose

This Policy sets out the guidelines for the usage of the services and data held within the R&R Data and Digital Service:

- In some instances, access to the Data and Digital Services will be restricted by the technology put in place to protect it; it is the Customers responsibility to refrain from circumventing or trying to circumvent these protective measures;
- It is the Customers responsibility to ensure that their behaviour meets the requirements of the R&R Acceptable Use of Digital Services Policy.
- It is the responsibility of all Customers to contribute to the security and safety of the R&R Data and Digital environment.

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, visitors or anyone else authorised to subscribe to the R&R Digital Service.

The method by which the R&R Data and Digital Services are accessed, for example via D&D supplied equipment or through a Customers own device, has no bearing on acceptance of this Policy. 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.

4 Exclusions

This Policy does not apply to those who use their own device AND are not connected to the R&R Digital Service in any way. In addition, it does not apply where a service or data is officially released to the public (e.g. via the dedicated website).

Any digital services and data held under the remit of the Parliamentary Digital Service (PDS) are independent of the R&R Digital Service and are monitored and audited by the standards and policies set by it.

5 Definitions

R&R 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 to the R&R Digital Service.
BYOD	Bring Your Own Device, equipment belonging to a Customer.

6 Responsibilities

6.1 Developing and Assuring the Policy

The D&D Team is responsible for maintaining and updating the Acceptable Use of Digital Services Policy. Individual roles within this team will provide specific expertise in areas including Cyber Security.

It is the R&R Digital Service Centre that will monitor and audit the R&R Digital Service to protect it and to ensure compliance with its usage. The team will continually monitor usage for abnormal or unusual activity and behaviour through observation and automated means.

Normally, the team will not manually inspect the content of voicemail, emails and other such communications. However, when there is a justifiable reason for performing such an inspection, it will be performed under controlled conditions to halt or contain a suspected cyber-attack or to perform the appropriate formal investigation.

6.2 Customer Responsibilities

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

- protecting all R&R data and information that they have access to,
- not attempting to remove, download or transfer R&R data to non-R&R environments unless expressly given permission to do so by the Senior Information Risk Officer (SIRO),
- abiding by their legal and regulatory responsibilities,
- upholding the R&R Acceptable Use of Digital Services Policy set out in this document,
- using the service for personal use providing that there is no infringement to the Policy,
- using the service for personal use providing it does not detrimentally impact the R&R Programme,
- reporting any suspected cyber security incidents to the Digital Service Centre, and
- reporting any breaches of the Customer responsibilities to the Digital Service Centre.

7 Policy Musts and Must Nots

By participating in and using the R&R Digital Service, the Customer agrees to abide and uphold the following:

7.1 Musts

Customers must:

- regularly complete the mandatory online cyber security awareness training,
- have an up to date understanding of basic cyber security threats and what you can do to counter them,
- only use accounts assigned to them,
- only use services that they have been authorised to use,
- notify the Digital Service Centre as soon as there is any change in circumstance that may require an alteration or revocation of access arrangements e.g. joiner, mover, leaver, promotion,
- upon first use, create a unique, strong password which is only known to them and in a format as directed by the Digital Service Centre,
- protect the R&R Digital Service from unauthorised access, loss and theft,
- must be vigilant and report any unusual digital activity/behaviour to the R&R Digital Service Centre,
- ensure that all devices and software/apps they use receive security updates in a timely way,
- only use reputable software and apps on their personal device when this device is, or could be used, to access the R&R Digital Service under a BYOD service,
- take all reasonable steps to maintain the security of any device that accesses the R&R Digital Service whether on R&R premises or elsewhere,
- present any media (e.g. USB memory sticks) to the Digital Service Centre for analysis **before** attempting to access them,
- follow the R&R Digital Service's cyber security advice and policies for overseas travel,
- be aware that the R&R Data & Digital Service is not responsible for the loss of data or information unconnected with the R&R Programmes work that is stored within its environmental remit,
- report to the R&R Digital Service Centre of any actual or suspected cyber security incidents (including virus infections, loss or theft of devices or information),
- report to the R&R Digital Service Centre any actual or suspected breaches of these Policy responsibilities, and
- provide full cooperation and support to any investigations performed by the R&R Digital Service Management.

7.2 Must Nots

Customers must not:

- use removable media, such as USB memory sticks, in any attempt to copy or move data from the R&R Digital Service without prior approval from the Digital Service Centre,
- share their passwords,
- allow anyone else to use devices on which you are currently logged onto the R&R Digital Service,
- override or undermine any security measures present on the R&R Digital Service,
- attempt to subscribe to or access Software as a Service (SaaS), i.e. web-based solutions, whose usage has not been authorised by the Data & Digital Service,
- carry out or permit any activity that may reasonably be regarded as unlawful, and
- hold or process any information that is classified at government SECRET or above.

8 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.

9 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.

10 Associated Documentation

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.

11 Equality Assessment

An Equality Assessment has been performed against this document and can be found in Equality Analysis Acceptable Use of Digital Services Policy available on the Vault or from R&R D&D Communications.

Sarah Johnson
CEO, Sponsor Body
September 2020

David Goldstone
CEO, Delivery Authority
September 2020