IT Systems Acceptable Usage Policy

Estates & Technology Services Department (ETS)

Introduction

The Royal Botanic Garden Edinburgh (RBGE) provides a variety of digital facilities to users. The ETS team ensure that RBGE's computing, and communication facilities, applications, data, network, and equipment are protected against loss, misuse, or abuse. This policy applies to all users which includes anyone with an RBGE account, including BTC staff; and provides a summary of what constitutes acceptable and unacceptable use of facilities. This policy document will be subject to regular review and updated to ensure compliance with current cyber resilience and information governance standards and RBGE's digital strategy.

ETS facilities are in place so you can carry out tasks which support RBGE's objectives and goals. It is important that there is an understanding that RBGE owns and is legally liable not only for the equipment and material, but also for any emails and content generated by or stored on its equipment. Digital facilities include any device belonging to RBGE or connected to any RBGE network, service, or system.

Any data created by RBGE users is subject to records management and GDPR policies and requires to be stored appropriately.

Although this document gives specific guidance, there are two principles which should guide any acceptable use of the facilities:

- Use must be lawful
- Use must not be to the detriment of other people or RBGE

Access Control

Access to the RBGE IT systems is controlled by usernames, passwords, and additional authentication techniques. All usernames and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all their actions on the RBGE IT systems.

If you suspect your password may have been compromised, you must immediately change it and notify the Service Desk.

You should not:

- Share usernames and passwords under any circumstances
- Leave passwords unprotected (for example, writing it down)
- Attempt to access data you are not authorised to use or access
- Multi-factor authentication (MFA) must be enabled for all users and all supported systems
- Connect any non-RBGE authorised device to the RBGE network or IT systems
- Store RBGE data on any non-authorised devices

A user's extent and limits of authority regarding access to digital systems and data should be discussed with your line manager in the first instance. Any amendments should be requested via the Service Desk and approved by the Information Asset Owner, this could be the file or folder owner.

Physical Security

To reduce the risk of unauthorised access or loss of information, RBGE requires the following:

- When signed in to RBGE systems, always use the screen lock facility. This includes setting a PIN or password on mobile devices
- Confidential material should be stored in a secured location, e.g., printed documents in a secured drawer, files stored in OneDrive and not on unencrypted removable media
- All business-related printed matter must be disposed of using red confidential waste bins or shredders

Data Protection

It is your responsibility to report confirmed, suspected or near miss incident data security breaches to your line manager, the RBGE Data Protection Officer and the Service Desk. You should read the data breach policy and complete a Data Breach Policy form. A data security breach means a breach in security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data.

You should:

- Understand that you and RBGE have a legal responsibility to protect personal and sensitive information.
- Ensure that all information is created, used, shared, and disposed of in line with business need and in compliance with the records management policy
- Not attempt to access personal data unless there is a valid business need that is appropriate to your job role

All breaches of this policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with RBGE disciplinary procedures

Internet, Email and Systems Use

Use of RBGE Internet and email is intended for business use. Any personal use should be agreed with your line manager. Personal use should not:

- Affect your performance
- Be detrimental to RBGE in any way
- Breach any terms and conditions of employment or RBGE policies
- Place you or RBGE in breach of statutory or other legal obligations
- Share device access to any non-RBGE users including members of your household

You should be aware that use of RBGE systems is monitored and, where breaches are found, action may be taken under disciplinary procedures. RBGE reserves the right to restrict or withdraw access to certain telephone numbers or Internet sites if we consider personal use to be excessive.

Occasional user awareness campaigns, including simulated phishing campaigns and cyber security training courses, will be sent at random intervals. Training should be completed at the earliest opportunity, especially if a simulated phish was successful, and any suspicious messages should be reported via the 'Report Message' button in Outlook. Any mandatory training, as determined by RBGE, must be undertaken at the earliest opportunity.

Monitoring of employee computer usage is lawful and will be carried out in accordance with audited controlled internal processes to ensure data security.

Users are accountable for their actions on the Internet and email systems, therefore should not:

- Use the Internet or email for the purposes of harassment or abuse
- Use profanity, obscenities, or derogatory remarks in communications
- Access, download, send or receive any data (including images), which could be considered offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material
- Use the Internet or email to make personal gains or conduct personal business
- Use the Internet or email to gamble
- Use the systems in a way that could affect its reliability or effectiveness
- Place any information on the Internet that relates to RBGE, alter any information about it, or express any opinion about RBGE, unless they are specifically authorised to do this
- Send unprotected sensitive or confidential information externally without authorisation
- Automatically forward RBGE mail to personal (non-RBGE) email accounts (for example a personal Gmail or Hotmail account).
- Make official commitments through the Internet or email on behalf of RBGE unless authorised to do so
- Download copyrighted material such as software, music, film, and video files (not an exhaustive list) without appropriate approval
- In any way infringe any copyright, database rights, trademarks, or other intellectual property

Accidental Access

You may unintentionally connect to websites that contain illegal or offensive material or pose a potential security risk. If this happens, you should disconnect from the site immediately and inform your line manager and the Service Desk.

If you receive an email containing offensive or suspicious material, report it via the 'Report Message' button in Outlook so that steps may be taken to avoid receiving further similar mail from the same source.

Remote Working

When connecting to the RBGE network from off-site the following controls should be applied:

- It must be in line with RBGE home working policy
- Equipment and media taken off-site must not be left unattended in public places or in sight in a vehicle
- Mobile devices should be carried as hand luggage when travelling
- Information must be protected against loss or compromise when working remotely (for example at home or in public places). Laptops should be locked and physically secured. They should not be

left unattended, and care should be taken to avoid 'shoulder-surfing' where people view your screen over your shoulder.
- Unsecured wireless networks, those that do not ask for a password, should not be used. If no secure network is available, an RBGE mobile phone can be used for tethering.
- Where possible, access files via OneDrive or remote access to RBGE systems to ensure that data is saved on RBGE systems.
- When on a video call, ensure there is no confidential information visible in your background. Blurred or virtual backgrounds can assist here.

Note: You must report all lost or stolen devices to the RBGE Data Protection Officer and the Service Desk immediately.

Data Storage

Cloud Services

All RBGE data must be stored on RBGE provided storage systems. In the case of cloud services, RBGE provides Microsoft 365 which includes OneDrive, Teams and SharePoint. Unauthorised applications, services or personal accounts should not be used to store any RBGE data. Any additional requirements must be discussed with your line manager and approved by ETS.

Mobile Storage Devices

Mobile storage devices such as USB drives, optical media, and external hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Any such devices must have encryption enabled when transferring sensitive or confidential data.

Software

Only authorised software should be used on RBGE computers. Software must be used in accordance with the supplier's licensing agreements. All software on RBGE computers must be approved by ETS prior to installation. Requests can be made to the Service Desk.

Users, where possible, should use software already available at RBGE. If the software does not have the required functionality a business case should be submitted to the Service Desk. This should include reasons why the software is required, who will use it and yearly costs that will be incurred.

Endpoint Security

ETS has implemented centralised, automated malicious software detection on all RBGE managed devices.

- You should contact the Service Desk immediately if you have any concerns around malicious software or cyber threats
- Desktops and laptops should be restarted regularly or when prompted to allow important updates to install

- You must not attempt to remove or disable endpoint security software

Telephones - Conditions of Use

You should not:

- Use RBGE phones for conducting personal business
- Make hoax or threatening calls
- Accept reverse charge calls, unless for business use

Further information can be found in the RBGE Mobile Device Policy.

Leaving RBGE

All RBGE equipment must be returned to your line manager on your last day of service.

Policy Owner: **ETS**
Last review: **Aug 2023**
Next review: **May 2024**