East Riding Archaeological Society

Device & IT Policy

May 2018

1. INTRODUCTION

1.1 The use of personal mobile devices, such as smartphones, laptops and tablets in connection with the East Riding Archaeological Societies' (ERAS) business is a privilege granted to specific officers of the Executive by appointment at the Annual General Meeting held in April or May every year.

1.2 ERAS reserves the right to revoke these privileges if Users do not abide by the policies and procedures set out in this policy.

1.3 These policies are in place to protect the integrity and effective operation of ERAS' data, information and communications systems to ensure they remain safe, secure and available for carrying out the ERAS' business, including:

- To protect devices and systems from downtime, caused by malware and viruses.
- To protect systems and information that is necessary to business processes, which would present risk to the operational requirements of the business.
- To protect information where access must be restricted to certain groups or individuals.
- To protect the value of the information to the Society e.g. intellectual property, commercially sensitive information.
- To protect confidential information because of legal obligations, such as personal data under the Data Protection Act or payment card PCI-DSS regulations.
- To protect information included in regulatory requirements, such as financial data
- To protect information that is externally owned or provided, such as those defined in contracts
- To protect information that is important to health and safety

1.4 This policy document covers the many areas, in a simple and concise format, which are necessary to manage and secure our IT and device environment.

2. USER ELIGIBILITY

2.1 The policy applies to all those that use personal devices and to consultants and other temporary workers, who require access to specific systems to carry out their duties.

2.2 ERAS may limit what data or systems can be accessed by personal owned devices.

2.3 Users with personally owned devices can access the following list of applications according to their role within the society, and the type of personal device: **Nationbuilder Website, ERAS Laptop computers, ERAS Samsung tablet, ERAS external hard drives, Dropbox, Facebook, Twitter, ERAS email accounts**.

2.4 The User must understand the consequences of installing personal applications on personal devices used to access information and

communications systems. These can introduce malware into systems, or result in exposing confidential data held, to theft or loss.

2.5 Best practise includes:
- Use only well-known and well-respected application vendors.
- Use any ERAS App repositories intended for personal devices.
- Maintain up-to-date security software on personal device(s).
- Automatically run/accept regular updates of the application software.

2.6 ERAS will permanently delete all its records of an inadvertent contact with a User's personal data and inform the User as soon as discovered and practical.

2.7 ERAS will never search a User's device data without the prior consent of the User.

2.8 If the User device has been contaminated with malware, which presents a risk to ERAS' data and its systems, then it has the right to wipe the whole device, which may result in the loss of personal and business data. ERAS will make every effort to communicate with the User BEFORE these actions are taken.

2.9 ERAS disclaims any liability for loss of personal applications or data, whether directly or indirectly resulting from the usage of company information and communications systems, and/or the wiping of company apps or data, or the removal of malware or the wiping of the whole device.

2.10 ERAS does not accept any financial responsibility for mobile phone, mobile data and public WIFI services incurred by the User.

2.11 The User is responsible for reporting lost or stolen devices or breaches of security on personal owned devices to the ERAS Data Controller in the first instance.

2.12 Upon leaving the Officer position the **User MUST** remove all ERAS information, applications, passwords, data and APPs from personally owned devices upon separation from ERAS or at ERAS' request.

2.13 ERAS may/will require checking and/or wiping of any company data held on personal devices.

2.14 ERAS owned, licensed and installed software on personally owned devices is required to be reconciled. Depending on the type of license:
- ERAS may request the User to reimburse the cost of the software, or
- ERAS may request the User destroy the software, or
- ERAS may decide to allow the User to keep software with no further value.

2.15 ERAS will not provide support for broken personal devices.

2.16 If the User circumvents configurations, security, access and practices then the User will be in violation of the this policy.

3. USER AGREEMENT AND RESPONSIBILITIES

3.1 **The User MUST** comply with the this policies terms and conditions.

3.2 **The User MUST** contribute to the protection of ERAS data, applications, information and communications systems by exercising caution, being aware of the risks, complying with security requirements and security best practices.

3.3 ERAS retains ownership of all the business data, documents and files, intellectual property and secure-access information and has the right and obligation to govern this data.

3.4 The User agrees that ERAS may require them to implement specific device configurations or software before the User is allowed access to data, applications, networks, information and communications systems. If the User disagrees with any of these requirements, they will not be allowed access from their own device(s), or may only gain access to certain systems, or may only be given guest access to the Internet.

3.5 ERAS and the User must comply with all regulations and laws. These laws and regulations might require the ERAS to access its data on your personal device(s), or you may be compelled to provide or remove any such data from your personal device(s).

4. ACCEPTABLE USE

4.1 **The User MUST** follow all administrative and acceptable use policies when a personal owned device is connected to ERAS networks, information and communications systems or where social media and/or collaboration solutions are applied for business purposes.

4.2 **The User MUST** ensure that when they use their personal device for personal reasons, that they are not using the ERAS intellectual property rights, any business confidential data, or any data that may be regulated or protected under European or UK legislation.

4.3 ERAS retains the right to perform operations on a personally owned device, such as scanning for malware, or checking security configurations. The User will be made aware of how and when these operations will be carried out.

4.4 Users who do not wish to have the required operations undertaken on their device, will not be allowed to access the ERAS networks, information systems, applications and data.

4.5 **The User MUST** consider the sensitivity of the ERAS data held on the personal owned device, when sharing the device with family and friends.

4.6 **The User MUST** report **IMMEDIATELY** any data breaches, disclosures or malware infections on personally owned devices to the ERAS immediately they become aware.

4.7 As a condition of access to ERAS data and ICT resources, the User is required to install security software.

4.8 The **User MUST** regularly update and/or accept updates to OS software directly provided by the devices manufacturer or service provider.

4.9 Jailbreaking, rooting and modifications to the personal device OS are **PROHIBITED**.

4.10 **The User MUST** back-up or synchronise any ERAS data/information held on their personal device with company systems.

4.11 **The User MUST** ensure that any device that is to be replaced or thrown away must have the permanent memory wiped.

5. LOGINS, PASSWORDS, PINS AND AUTHENTICATION

5.1 ERAS will issue Logins and Passwords for access to its network, applications, information and communications systems - as it does with company-owned devices. This information **MUST** never be passed on to third parties or communicated on personal social networks.

5.2 The User **MUST** ensure there is a PIN or Login to operate any personal owned devices before access to ERAS networks, information systems, applications and data can be granted.

5.3 ERAS may require device PINs and passwords to be changed regularly, to comply with its security policies, regulatory or legal requirements.

5.4 ERAS may enforce the use of passwords for personal owned devices to comply with its policy or any data governance.

5.5 ERAS may block USER access for those with out-of-date passwords, or passwords with a low strength.

5.6 Where the ERAS uses additional security techniques to secure its data and systems, such as two-factor authentication, the User **MUST** use such systems with their personal device where directed.

5.7 The User has a responsibility towards the safeguarding of company and confidential data in their possession. It is best practice to encrypt confidential data on mobile devices in case of loss or theft.

5.8 If a User does not want their personal device to be managed or have policies enforced, then they may/will not be allowed access to the ERAS network, information and communications systems, or the User may be given limited access to company systems.