UNIVERSITY OF PORTSMOUTH

TRANSFERRING RESTRICTED DATA BY EMAIL

March 2021

Contents

Document title
Transferring Restricted Data by Email
Document author and department
Rob Walker - Information Services
Approving body
IS Board
Date of approval
4 April 2021
Review date
April 2022
Edition no.
1.0
ID Code

A180473	
Date of effect	
See approval date	
EITHER For public access online (internet)? Tick as appropriate	**NO**
For public access on request copy to be mailed Tick as appropriate	**YES**
OR For staff access only (intranet)? Tick as appropriate	**YES**
Password protected Tick as appropriate	**NO**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk If you need this document in an alternative format, please email corporate.communications@port.ac.uk	

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

Email is not a secure means of communication. Sending a message by email is a bit like sending a postcard - your message could be read by anyone who handles the card during its journey through the postal system. Similarly, anything written in an email can, in theory, be intercepted and read by any so-called '*man in the middle*'. A further risk arises because it is easy to send an email to the wrong person by accident. Encrypting the message contents provides a solution to these risks. This IS advisory sets out the secure procedures which must be followed when sending restricted information (e.g. personal data or commercially sensitive information) by email.

Who is this for?

This advisory is aimed at all members of the University of Portsmouth including third party contractors.

How does the University check this is followed?

Annual review of this advisory will be performed to evaluate its relevance and effectiveness.

Who can you contact if you have any queries about this document?

Any questions about this advisory should be directed to servicedesk@port.ac.uk

1.0 Introduction

One of the earliest email systems was used at Massachusetts Institute of Technology from 1965. Only after email started to become well established in the mid 1990's did issues of security and privacy begin to emerge. Since that time there has been a constant battle to make email 'safe' - even though it was never really designed to be.

2.0 Risks

2.1 Email is not private

The sender of an email must understand the nature of the information it contains so that the risk of a data breach can be assessed and the appropriate security safeguards applied.

2.2 Email cannot provide security at the destination

Email simply transmits the information; it cannot provide security at the destination. The sender must ensure that adequate security controls are applied to the information at its destination. The sender must be confident that the information will be read/processed by the intended recipient and authorised individuals only.

It is important to obtain an assurance in writing from the intended recipient before the information is sent.

2.3 Email can be forged

Fraudsters, thieves and con-artists use email to trick the unwary into revealing valuable information. It can be hard to tell a genuine email from a bogus one. The University has security controls in place to prevent email address spoofing - but no security measure is 100% effective.

2.4 Email will go where you send it.

If you mistype an address and press send then it's almost impossible to fetch it back.

You must have a legitimate business need for sending **Restricted** information by email. Ensure that there is a legitimate business need to send this information and have this authorised or confirmed in writing by a line manager. If the information must be sent, consider sending the minimum necessary for the purpose (e.g. a synopsis, edited or redacted version).

If it must be sent, then the contents must be encrypted. If you mistakenly send encrypted data to the wrong destination then it's not a complete disaster because the information cannot be read without a password.

3.0 File encryption - for security ‘in transit’

3.1 Encrypt the file or folder (using the built-in features of MS Office or an approved encryption tool). Contact Information Services if you need help with this.

3.2 Attach the encrypted file to an email (disclose as little as possible about the contents of the encrypted file in the message text).

3.3 Send the email with the encrypted enclosure.

3.4 Send the password to unlock the file - “out of band” - **i.e. over a separate channel known only to you and the intended recipient (e.g. SMS text message, letter, telephone call).**

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk