UNIVERSITY OF PORTSMOUTH

SAFE SHARING OF ADVANCE PASSENGER DATA

May 2015

Contents

Summary 5

- What is this document about? 5
- Who is this for? 5
- How does the University check this is followed? 5
- Who can you contact if you have any queries about this document? 5
- 1.0 Fundamental Principles 6
- 2.0 Sharing Advance Passenger Information (API) data with travel service providers 7
- 3.0 Security of personal data required by the travel service provider 7
- 4.0 Service provider responsibilities under the Data Protection act 1998 8

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
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

What is this document about?

It may be necessary to share personal data - identifying students and some staff - when arranging field trips or other forms of educational travel.   For example, sharing Advance Passenger Information (API) data with travel service providers. This advisory of sets out best advice for securely sharing personal data in this context.

Who is this for?

This IS Advisory is aimed at staff and students of the University of Portsmouth who are planning, arranging or taking part in educational travel.

How does the University check this is followed?

Annual review of this IS advisory will be performed to evaluate its 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 Fundamental Principles

1.1 API data should be only shared on a clear 'need to know 'basis and appropriate access control permissions must be set to allow only staff involved in the arrangement of field trips to have access to API data.

1.2 Staff involved in the arrangement of field trips must not make personal copies or share these documents or information with others.

1.3 Staff needing access to the API data (i.e. those involved in the arrangement of field trips) must protect their University Google Apps account with 2-factor authentication. Information Services can give advice on how to activate this security feature. *This is especially important if staff need to access data from a remote location or when using a mobile device.*

1.4 Staff using a mobile device or smartphone to access personal data must activate all available security features to protect the data (e.g. use a PIN code or password to lock the device). Contact Information Services on ext 7777 for assistance.

1.5 Students must be made aware that their personal data (including name, date of birth and passport details) will be collected and stored on a University Google Drive and University based digital storage, subject to the following security controls:

1. their data will be encrypted.
2. their data will only be accessible to staff that need to know
3. unauthorised copies of the data will not be made.
4. their data will be deleted when its storage is no longer necessary.
5. all available security features offered under Google Apps will be applied.

1.6 Students must be told who they can contact if they have any concerns.

1.7 Data will only be made shareable while the need to share exists. **The greatest care must be taken when sharing data - check names carefully and confirm that the data will only be accessible to authorised staff.**

1.8 After completion of the field trip and payment to service providers, the API data may be kept on the Google Drive for up to one year.

1.9 Only data from the most recent trip will be retained. This will be used to inform future trips and to solve any disputes with service providers or settle insurance claims; older data will be deleted at the end of the following academic year. Associated emails will be labelled according to trip and year and deleted at the end of the following academic year.

2.0 Sharing Advance Passenger Information (API) data with travel service providers

2.1 Students should be made aware that in the process of booking travel services, their personal data will be made available to approved travel service providers. Travellers will need to provide Advance Passenger Information (API) before the journey. This data is required by carriers and is also called: **APIS, Secure Flight or e-Borders.** This is passport information that is required by the government of the destination country. Many airlines also need this information for aviation security purposes. API includes, but is not limited to:

- Full name (last name, first name, middle name if applicable)
- Gender
- Date of birth
- Nationality
- Country of residence
- Travel document type (normally passport)
- Travel document number (expiry date and country of issue for passport)
- [For US travellers] Address of the first night spent in the US (not required for US nationals, legal permanent residents, or alien residents of the US entering the US)
- Dietary requirements
- Next of kin contact details

3.0 Security of personal data required by the travel service provider

3.1 API must only be supplied to the travel service provider in the form of an encrypted document attached to an email. The password which secures the API attachment must be sent separately (i.e. the sender must contact the travel service provider by telephone, check that their email has arrived and only then provide the provider with the password). The password **must not** be sent by email.

3.2 Online entry of API data must be sent securely over an encrypted SSL connection between a web server and a browser.

4.0 Service provider responsibilities under the Data Protection act 1998

4.1 Any travel service provider employed by the University must provide a written undertaking that any personal data identifying students and/or staff will be adequately protected from loss, damage or unauthorised exposure while that data is stored by, or otherwise in the possession of the provider, or during any subsequent transit to or from the provider and any third party. This undertaking can take the form of the data protection statement published by the service provider.

The University department organising the travel must ensure that this undertaking is obtained from the travel service provider.

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