Policy on use of IT Equipment and Data Access Abroad

Document Control

Document Details

OWNER	Stephen Menzies / Alexander Cowen
APPROVER	IGG - TBC
CLASSIFICATION	Internal Use Only
DATE OF ISSUE	26/06/2024
ISSUE	v0.1
REASON FOR ISSUE/UPDATE	First Draft
NEXT REVIEW	06/2025
DISTRIBUTION	All Slough Borough Council staff

Revision History

VERSION	AUTHOR	DATE

This document outlines the policy for using IT equipment and accessing council applications and data while travelling abroad.

It aims to ensure that the council complies with the relevant laws and regulations on data protection and security, and that the council's data and systems are not compromised or misused.

Scope:
This policy applies to all 'employees' of Slough Borough Council and Slough Children's First who use IT equipment and access council applications and data while travelling abroad for work purposes. Please note taking work equipment abroad for personal reasons is not permitted unless authorisation has been sought from your line manager, director, DPO and HRBP.

The definition of 'employees' in this policy includes:

- permanent staff,
- elected members and commissioners,
- contract staff,
- volunteers, partners and other third parties who work on behalf of the council or have access to council data.

IT equipment includes laptops, tablets, smartphones, and any other devices that can store or access council data. Council applications and data include emails, documents, databases, and any other information that belongs to the council or is processed by the council.

Policy:
The policy is based on the following principles:

- IT equipment and data access abroad **must comply with the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018**, as well as any other relevant legislation and guidance.
- IT equipment and data access abroad must adhere to the government data classification scheme and the council's information security policy and procedures.
- IT equipment and data access abroad must be limited to the minimum necessary for the work purpose and the duration of the travel.
- IT equipment and data access abroad must be secure and protected from loss, theft, damage, unauthorised access, or misuse.
- IT equipment and data access abroad will be subject to regular monitoring and audit by the council's IT service and the DPO.
- IT equipment and data access abroad must be in accordance with the council's code of conduct and values, and respect the privacy and rights of individuals and organisations.

Authorisation to use IT equipment or access data whilst abroad (EU only)
The use of IT equipment and data access abroad must be authorised by the employee's line manager and the council's Data Protection Officer (DPO) before the travel takes place.

Any loss or theft of IT equipment and unauthorised data access abroad must be reported to the council's IT service desk and the DPO as soon as possible in case of any incident or breach.

Acceptable use EU/ outside EU
In line with its legal obligations around data protection and ensuring that the council's devices and data remain secure, the council has adopted a policy which restricts the use of council devices and access to data and applications whilst working abroad.

The Information Commissioner's Office (ICO) has outlined a list of countries and territories where data adequacy regulations are in place. The regulations outline a process whereby participating countries and territories share the same or similar levels of data security regulations and requirements to those required within the UK.

The countries noted below meet the ICO requirements:

1. European Economic Activity (EEA) states:

- Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

2. The European Free Trade Association (EFTA) states:

- Iceland, Norway and Liechtenstein.

3. Other countries and territories which meet the adequacy regulation requirements:

- Andorra, Argentina, Faroe Islands, Gibraltar; Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

Approval for acceptable use abroad
Within the countries or territories listed above, the use of IT equipment and data access is acceptable, subject to the above principles and the approval of the line manager and the DPO. However, access to data must be through the council's virtual private network (VPN) to ensure a secure connection and encryption of data.

Outside the list of acceptable countries and territories, the use of IT equipment and data access is not permitted, unless there are exceptional circumstances and a specific risk assessment and mitigation plan is agreed by the line manager, the DPO, HR and the relevant senior manager.

The line manager will need to accept any additional costs accrued during this period which may be applied if data roaming is enabled during this time. It is their responsibility to put into place any recharging of this to the employee.

The use of data outside of the UK must pass the ICO's checklist for the international transfer of data before this is approved.

Failure to comply with this policy may result in disciplinary action, up to and including dismissal, as well as legal consequences and reputational damage for the council and the employee.

Information Technology Department will:

- Provide support and advice on this policy via the IT Service Desk, Call the IT service desk on 01753 944199 Or Email ITServiceDesk@slough.gov.uk
- Maintain and manage Slough Council's security infrastructure, such as firewalls, and implement intrusion detection and prevention practices in order to limit threats and provide early detection of security breaches where possible.
- Monitor endpoint device connectivity and activity as it relates to managing and protecting the Council's network.
- Any exemption approved does not prohibit IT from disconnecting or isolating such devices if they are shown to be causing harm to the confidentiality, availability or integrity of Slough Borough Council's Information Security.

Related policies

Acceptable Use Policy

References

A guide to international transfers | ICO