

Personal Information Security Policy

IT Policies

Contents

Introduction	3
Implementation of Policy	3
GTI Laptops	3
Removable media (e.g. USB flash drives, CDs, DVDs, portable HDD)	3
Non-approved personal communication devices (e.g. mobile phone / PDA).....	4
Approved secure personal communication devices (e.g. mobile phone / PDA)	4
Non-GTI personal computers (e.g. home computer)	4
Backup tapes	5

Introduction

This is a statement of policy about the treatment of electronic information that is removed from British Council premises. It is intended to assist our flexible approach to working away from the office whilst acknowledging the risks associated with removing corporate information from our secure internal information systems. It explains the steps we have put in place to ensure the integrity of our information.

The organisation fully understands the need to transport devices containing information between permanent or temporary places of work or to send devices containing such information to partners in other organisations. It regulates the methods used to move information in order to manage the risks associated with the loss of devices containing information.

The driver for this policy is the directive from the UK Cabinet Office instructing public bodies to encrypt all personal and sensitive information that is taken outside the organisation's premises. We are required to comply with this instruction, which will remain in place until further advice is issued from the Cabinet Office. The British Council acknowledges that it is often difficult to interpret the definitions of personal and sensitive information provided to us and that the British Council does not formally classify information in the same way that government departments do. GIS has therefore sought way to reduce the burden of decision on colleagues whilst providing standards for the movement of information.

This policy applies to data that is taken or sent outside the corporate environment. Information within the corporate environment is classed as "information in our offices and private network, including our internal e-mail system".

Implementation of Policy

We have identified a number of different devices on which it is likely that colleagues will store information and addressed how we will treat the use of these devices in the future.

GTI Laptops

Statement: Encrypt all information on all laptops

Policy: All GTI laptops that are taken out of BC offices must use encryption for all major information types.

Rationale: Use of laptops while away from BC premises is important to our preferred business model of less dependency on premises-based activities and the ability to access all business information while working away from a BC office. GTI laptops automatically synchronise e-mail and files which means the user is unaware of the existence of personal information on their device. We want to be in a position where staff can use their laptops away from an office in a manner that does not compromise any personal information held on the laptop.

Approach: Global IS will apply an encryption solution that will automatically encrypt all information on a laptop. The encryption process will happen automatically in the background in a way that limits impact on normal laptop performance.

Removable media (e.g. USB flash drives, CDs, DVDs, portable HDD)

Statement: All removable media must be encrypted using approved products.

Policy: All information that is transported outside British Council offices using a medium such as USB stick, CD, DVD or portable Hard Disk Drive (HDD) must be protected by encryption with password protection.

Rationale: Given the British Council's globally disperse operating environment and our preferred business model of greater emphasis on delivery of products and services away from our premises – information transfer using removable media is an essential tool. If any

information were lost in transit in this way, it could cause embarrassment to the British Council or to others. We must be in a position where we are certain that all personal information on all portable media devices leaving British Council offices is encrypted.

To reduce the burden of choice of whether to encrypt or not, all removable media devices must be encrypted. The Cabinet Office's recommended option is to use hardware encrypted USB devices of a particular specification for information transfer and this is our preferred approach. However Global IS understands that transfer of information by USB memory stick is not always suitable, for example, where the media is being sent outside the organisation or is too large. In such cases CD-ROMs, DVDs, SD cards and Portable HDDs are acceptable, as long as approved encryption methods are used.

Approach: Global IS has identified USB sticks that have full disk encryption using AES 256-bit encryption. These are advertised on the Global IS intranet pages and must be used where possible. Other portable media used to transport information away from British Council premises must be encrypted using WinZip. View the WinZip user guide for more information on encryption standards.

Non-approved personal communication devices (e.g. mobile phone / PDA)

Statement: No synchronisation of information, copying of files, or forwarding of email to any devices in this category.

Policy: No information is to be synchronised, forwarded, copied or transferred to portable communication devices, including those that have previously been approved for this activity.

Rationale: Personal communication devices can automatically synchronise e-mail and files which means the user is unaware of the existence of personal information on their device. We want to be in a position where staff can use their mobile phones and PDAs away from an office in a manner that does not compromise any personal information held on them.

Approach: No personal communication devices or mobile phones are allowed to connect to the corporate network, synchronise, forward, or copy information from the network or PCs.

Approved secure personal communication devices (e.g. mobile phone / PDA)

Statement: Global IS will consult with the business in order to understand the full requirements for synchronising and copying information to mobile communication devices.

Policy: Currently no policy exists as there is no formal business case.

Approach: As soon as we establish requirements and a business case we will investigate the options.

Non-GTI personal computers (e.g. home computer)

Statement: All information to be saved on encrypted media using approved products.

Policy: While using non-GTI computers to access or work on corporate information using remote access tools such as ROAM all files must be saved to encrypted media as described above.

Rationale: Use of computers whilst away from BC premises is important to our preferred business model of less dependency on premises-based activities and the ability to access all business information while working away from a BC office. We want to be in a position where staff can use their home PCs to access information in a manner that does not compromise any personal information they may be working on. In order to reduce the burden of choice of whether to encrypt or not all corporate information on non-GTI computers must be encrypted regardless of where it is saved.

Approach: Global IS has identified software that meets our requirements for AES 256-bit encryption. View the WinZip user guide for more information on encryption standards.

Backup tapes

Statement: Ensure methods of moving tapes meets good practice, particularly overseas.

Policy: All backup tapes should be kept secure when being transported off-site.

Rationale: It is generally accepted that, although backup tapes contain all the information from our IT systems, they are held in a format and on a medium that would not readily be accessible to any third party unless they had specialist equipment.

Approach: Records should be kept of all tape movements to ensure that all tapes sent from one site arrive at their destination. Where appropriate, approved couriers should be used. Local risk analysis should be undertaken to gauge the impact of losing of such information and in high-risk locations extra security measures should be considered. The security of our backup tapes is the responsibility of the country director.