

Use and Misuse of IT, Communications and Systems

Introduction

BDP is responsible for maintaining the confidentiality, integrity and availability of the information it holds. To that end BDP invests heavily in information technology and communications equipment. These facilities are made available to staff for the purpose of BDP's business and must be used in a professional manner in line with all BDP policies and guidance.

The flexibility and freedom of communication provided by information technology is considerable, but this also presents opportunity for misuse of this valuable company resource. The information below highlights some areas of potential misuse, although this is not exhaustive.

Misuse of BDP's IT and communications equipment and facilities is regarded as a serious disciplinary matter and will, in some circumstances, be treated as gross misconduct, justifying immediate dismissal. If you are in any doubt about your responsibilities and obligations in any particular situation you should consult immediately with your local office IT representative.

Misuse of computing and network facilities and unacceptable behaviour includes (but is not limited to) the following:

- Attempting to gain unauthorised access to a facility, file server or any other IT service that you would not normally be expected to access during your day to day duties
- Making or viewing offensive material available over the network or internet
- Generating, sending, receiving or viewing pornographic material
- Giving your username and/or password to someone else, or being otherwise careless with them
- Stealing, using, or disclosing someone else's password without authorisation
- Generating messages which appear to originate from someone else, or otherwise attempting to impersonate someone else
- Sending messages or materials which are abusive, discriminatory, harassing, threatening, a nuisance, distressing or in breach of [BDP's Equal Opportunities and Dignity at Work policy](#)
- Software piracy (including infringement of software licences or copyright provisions), this extends to holding pirate or 'cracked' software on BDP's network or on any portable media devices connected to BDP's network
- Using IT facilities for commercial gain without explicit authorisation
- Physically damaging or otherwise interfering with BDP IT facilities
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Downloading, installing or copying software and electronic files that are copyrighted, or without authorisation
- Pirating software or storing pirated software on a BDP asset
- Sharing confidential material, trade secrets, or proprietary information outside of the organisation.
- Hacking into any website
- Sending or posting information that is defamatory to the company, its products/services, employees and clients
- Introducing malicious software onto the company network and/or jeopardising the security of the organisation's electronic communications systems
- Passing off personal views as representing those of the organisation
- Use of Proxy avoidance sites or services
- Streaming of internet radio and video unless explicitly permitted for business activities

The matters listed above extend to: BDP's IT infrastructure, desktops, laptops, smartphones and tablet devices whether used off network or connected directly to the BDP wired or wireless networks or utilising data services from our or other communications providers.

Purpose

The purpose of this policy is to:

- Ensure the confidentiality, integrity and availability of BDP's information assets
- Confirm how users should operate the systems provided to them
- Confirm how users should behave when using BDP systems
- Provide guidance and remove ambiguity in the compliance of this policy

Scope

The policies and procedures in this document are applicable to all BDP employees, both permanent and contract at all BDP's offices. They are also applicable to consultants working on behalf of BDP who have access to BDP information.

Use of BDP Devices

All BDP computers have local drives which hold the operating system, software and desktop. However, it should be noted an excessively full drive may reduce performance of the computer. Users should also be aware that at times there may be a requirement to move PCs and laptops from user to user at short notice and additional software might need to be installed, resulting in the removal of files without prior notice.

BDP does not take responsibility for any loss of any personal data whatsoever held on local drives.

Work related information should not be held on local drives except in certain circumstances agreed by Central IT or local office IT representatives (e.g. Laptop users might be required to take project data out of the BDP network or might need to create new data if working away from the office for a prolonged time). If this is required additional measures can be put in place to ensure the resilience of data, it is the users responsibility to highlight any such instance to IT representatives well in advance of any travel. On returning to the office the files **must** be moved back to the network or in the case of prolonged use away from the office then the files must be backed up to an external source.

BDP does not normally back up local drives on laptops or desktops.

Your network account provides logon access for your BDP device to a number of network drives that are for BDP work related use. You should familiarise yourself with these drives and what information should be stored on each.

No personal data (e.g. personal music, video and photographs) should be stored anywhere on computers provided to you to deliver work on behalf of BDP or on the BDP network, including your H: drive (home folder), which is private and should be used to store documents of a more confidential nature.

BDP does not take responsibility for any loss of personal data held on network drives and reserves the right to delete such files without prior notice.

To protect BDP information, users should always make sure their screen is locked when they are away from their desks.

If any user finds themselves able to access other user's data (including H: drive) then they must report the occurrence to their local IT representative or Central IT immediately.

Laptop computers must be locked away when not in use. This rule applies whether the laptop is with you at work, at home, or in the car. Laptops which are not securely stored must not be left unattended as this will invalidate BDP's insurance cover and could compromise the security of the device.

Users of smartphones and tablets that access BDP systems, whether provided by the company or not, have a responsibility to keep their devices secure at all times. These devices can synchronize email, contacts and calendars and have the ability to store other important and commercially sensitive

material. These devices must have a 6 character password enabled at all times and fingerprint recognition enabled where available.

Any loss of such devices must be reported to your local IT representative or Central IT as soon as the loss is noticed. Central IT will then disable or wipe the device.

Each BDP employee is provided with a phone number and either a softphone or a handset. BDP recognises that it will on occasion be necessary for staff to receive and make private calls. However, private calls should be restricted as far as possible to those matters which cannot be addressed outside of normal office hours.

Staff should be aware that all incoming and outgoing calls are logged and voicemail messages stored as part of the regular email backups. Whilst these are not regularly reviewed this information can be made available should the need arise.

Please be considerate when using mobile phones. The ringing tone should be set at a low level to avoid undue distraction to colleagues. Logs of all calls made from BDP provided mobile phones are included in invoices provided by BDP's mobile contract supplier. Whilst these are not regularly reviewed this information can be made available should the need arise.

Procedures for making a formal record of telephone conversations or mobile phone text messages of any significant job-related topics are described in the Design Process procedure for Project correspondence.

Use of non-BDP Devices

Employees, contractors and visitors to BDP may connect a non-BDP device to our network only in order to receive an internet connection. This will be by request and will be on an isolated VLAN which will be monitored to the same degree as the main BDP network.

Full network access by a non-BDP computer (i.e. access to network drives, data and printers) will not be permitted.

Employees may use their personal smartphone / tablet to access BDP email and Planet, unless specific project requirements prohibit this.

On no account should a BDP employee connect a personal device to the BDP Visitor Wi-Fi.

Internet Use

Access to the internet is provided for staff to search for material that is relevant to their work. Any web browsing should be limited to work related topics and any material downloaded to our networks must also be work related.

Reasonable personal use of the company's internet facility is permitted but should be limited to outside normal working hours. Internet sites are filtered for inappropriate site content and may therefore be blocked. Whilst home or hotel internet connections may not block sites that are unavailable from the BDP network our IT systems ensure that internet use is still recorded and will be monitored when next connected to the BDP network.

BDP monitors user activity on the Internet at network level for the purposes of security and integrity of the BDP network. This extends to PCs, laptops and personal devices connected to the BDP network both wirelessly and on occasion through wired connections. Monitoring also continues of BDP devices when used remotely, with user activity automatically reviewed when devices are next connected to the network. This includes user identification (SSID and IP address), domain names of websites visited, duration of visits, and all files downloaded from the Internet. Staff should be aware that this monitoring may reveal sensitive data about them, for example visits to websites which detail the activities of a particular political party or religious group might indicate the political opinion or religious belief of that individual. Staff should maintain their own personal privacy by not using BDP's systems

to access this type of information. Staff should also acknowledge that all internet activity logs are regularly backed up with records maintained as necessary for the stability and robustness of BDP's overall IT systems.

It is important to note that BDP policies, including this one, apply to all BDP supplied devices (laptop, smartphone, tablet) whether used inside or away from the office and any personal devices connected to any BDP network.

It is imperative that our IT policies are adhered to at all times.

Inappropriate use of the internet may result in disciplinary action.

User Accounts

All BDP employees are provided with a personal network username, password and email address. The password is personal to you and must conform with and be changed in accordance with our password policy. You should not disclose your password to others by any means unless requested to do so by an authorised BDP IT Administrator.

BDP is aware of its responsibility to not infringe the privacy of individuals in the workplace. However, as permitted by relevant legislation, we undertake continuous monitoring of the use of all IT facilities, including home areas and internet sites visited, to ensure there is no breach of BDP policy.

There will be occasions when the company will need to unlock computers and change user passwords without the user's permission.

Email

All email messages (outgoing and incoming) are recorded, are stored in line with our retention policy, have a copy made of them and are replicated/backed up for disaster recovery purposes.

Once an email is sent, there is very little chance of retrieving it. If a mistake has been made, the resultant damage may be magnified because of the possible widespread nature of the distribution. This gives rise to a number of legal risks for companies.

Email messages, unless protected by privilege, must be disclosed to the other side in a court action if relevant to the issues in the case. Therefore, it is important for companies to adhere to recognised procedures.

All emails sent externally from BDP contain a legal and commercial disclaimer, which is automatically attached by the company's systems and confirms that the message and attachments are sent on behalf of the company for the purposes of the business.

The following are the key issues that all staff must be aware of with regard to the use of email:

- Email messages, even if they are meant for 'one to one' personal use, should be treated in the same way as more formal methods of communication e.g. letters. Content and language used must be of a standard that could be issued to any member of staff or to a client. It must be remembered that any email could be accidentally, or maliciously, forwarded to an external party or to anyone on the BDP email system
- The content of email is subject to all laws such as those relating to copyright, defamation, data protection and public records as well as statutes concerning the sensitive issues of harassment and pornography. Any statements made by employees that could be construed as racial or sexual harassment, libellous, or in breach of confidentiality, offensive or slanderous will attract both corporate and personal liability and disciplinary action
- An employee should not breach company confidentiality by disclosing information of a confidential nature through the company email system
- The email system can be used to announce official BDP events but should not be used to promote individual sales of goods nor should it be used to make social or domestic

announcements. Other means of communication exist to facilitate this i.e. notice boards and on your local 'Studio' section on Planet

- An email message may contain or attach a copyright work owned by a third party. It is an infringement of copyright to make an electronic copy of such work even if it is only transient
- The use of BDP's email systems for personal email should also be avoided as all email traffic is captured and backed up automatically without differentiation between business and private communications

Further guidance on communication by email is provided on the BDP ['email etiquette'](#) page.

Instant Messaging (IM)

BDP has adopted IM to simplify the communication of short messages in lieu of using email. In general IM will be less formal than email, but should still use proper language and content to maintain professionalism.

Employees must be aware of the risks that can contribute to the legal liabilities of the company when communicating using IM.

IM must not be used for any external communication (unless to an authorised federated partner) where this needs to be documented, recorded, or saved.

IMs are archived in the same way that emails are currently archived.

When using IM follow these BDP company guidelines:

- Be brief. As a general rule an IM should be no more than a sentence or two. Save longer conversations for meetings, conference calls or emails.
- Don't use IM as a substitute for serious, sensitive, confidential or contract related communications i.e. to negotiate contracts, place orders, make or commit to important decisions. If an IM is moving in that direction then suggest a face to face meeting / web conference or email.

Software

Most software requires BDP to have a licence for each software installation. Failure to adhere to software licence agreements could lead to BDP facing legal action, therefore, only authorised, correctly licensed software may be run on BDP PCs.

Software, including free apps and trial downloads, should not be installed unless directed to do so by your local IT representative or Central IT. As part of your role, particularly if travelling abroad, you may be given temporary privileges to install applications; however, this should not be abused.

USB Portable Storage Media

BDP recognises that from time to time portable USB storage requires to be used for business purposes. Our systems automatically scan devices to ensure they are not going to introduce any threats into BDP's system. Should any virus be detected the USB device should immediately be removed from the PC or Laptop.

Staff using portable storage media should also be aware that all files modified or written to such devices are automatically logged by CIT, recording; User, Date / Time, Files written, and original file location. These logs are reviewed on a weekly basis with any abnormal behaviour investigated and potentially addressed through BDP's Disciplinary Procedure.

Responsibility for the Policy

For the purposes of this policy, the Director of Information, Technology and Process will have primary responsibility for the regular review and update where appropriate. The responsibility for the appropriate and effective application of the policy across each studio is with the Studio Chair (UK) or Studio Leader (International).

This is BDP's Use and Misuse of IT, Communications and Systems policy and as chief executive I commit myself and the company to it.

Signed

A handwritten signature in black ink, appearing to read 'John McManus', with a stylized flourish at the end.

John McManus

Chief Executive

Date: 2 January 2019