bpArchitecture

01782 515555
enquiries@bparchitecture.co.uk

Security & Confidentiality Policy

This policy covers security of information and data held by bpArchitecture (including IT hardware, software and data) and all aspects of confidentiality relating to the work of the practice.

Scope

This policy covers:

- All staff employed by or contracted with bpArchitecture
- All personal computers (desktop machines, laptops and hand held computers including iPhones, IPads and other similar devices), attachments and software owned or leased by the practice, whether used at home or within the work place, including practice software installed on personal devices.
- All servers and other hardware and software required to run the networks and information systems
- All work files and confidential information used by or about employees, clients, consultants and contractors

The Data Protection Act covers all identifiable data held on any system (manual or electronic).

Intention

This policy supports procedures that promote security and confidentiality but does not restrict people's ability to work. For example, the need to lock dektops or log off the network when leaving the desk has been weighed against the time taken to log back on. The risk of someone else accessing the network and the likelihood of damage has been considered when devising this policy and security must be appropriate to the risk. Any significant risks identified must be recorded and quantified.

All sections of this policy have been written to ensure that security and confidentiality is maintained whilst allowing the work of the practice to be carried out and completed practically and efficiently.

Policy Review

The policy will be reviewed regularly, either as part of the standard annual review of all bpArchitecture policies, or sooner if required. All staff will be informed when the policy is updated. The policy is filed on a shared network drive, and all Directors and staff will have access to a paper copy (kept in the Office Library). All policies are also available on the practices Intranet site .

Legislation and Guidance

Under the guidelines training must be provided for all staff and updated as necessary.

Data Protection Act

The Data Protection Act 1998 applies only to living individuals and requires:

- A named lead to manage data protection compliance within the organisation. Beverley Poole is the named lead for data protection compliance within the practice
- Internal training, current awareness and updates

British Standard BS7799

This is the British Standard relating to security issues around the use of IT in all areas of business.

Other

There is other legislation that affects information governance including inter alia, the Human Rights Act and the Electronic Communication Act 2000 together with guidelines and codes of conduct from various bodies including inter alia, RIBA, CIAT, MRTPI, CIOB, CIArb. bpArchitecture are committed to keep up-to-date on any developments in these and other information governance areas.

Policy Responsibility

Staff Responsibilities

The Practice Principal has overall responsibility for security and confidentiality issues within the organisation.

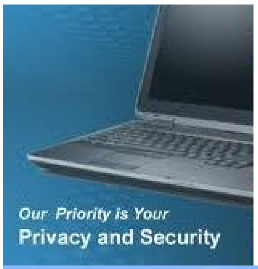
Members of the team who manage or supervise staff are responsible for ensuring their staff are aware of the policy and are adhering to the policy. Each individual member of staff is personally responsible for ensuring their use of computers, software and confidential information adheres to this policy.

Induction & Training

- The named lead for Data Protection Compliance will induct new staff when joining the practice so that they are aware of the policy and what actions they need to take to work in line with this policy.
- All staff will sign an authorised user compliance form when joining the Practice (including trainees and students).
- All staff will sign an appropriate declaration covering use of laptops and other equipment when out of the office.
- Re-fresher training sessions covering the policy will be given annually, or more frequently in the event of significant changes in the policy. All staff must attend these sessions.

Leaving Procedures

- Whenever a member of staff leaves, any relevant security system codes should be changed and all keys, passes etc should be handed in.
- The leaving procedure, including the network leavers form, must be worked through, completed and signed.



Code of Conduct

All staff of bpArchitecture must understand and comply with their professional Code of Conduct be this ARB, RIBA, or CIAT or other professional body.

Breach of Policy

All staff of bpArchitecture should sign a declaration which makes reference to this policy and this will be binding. Breach of any part of this policy will be a serious disciplinary offence.

- Any breaches of this policy will be reported to the Principal
- Anyone suspecting a breach or discovering a situation where a breach could occur should discuss this with lead for Data Protection.
- Deliberate passing of confidential information to unauthorised people is a disciplinary matter which may lead to dismissal.

Internet use is monitored. Inappropriate use of the internet or the sending of inappropriate emails will result in disciplinary action and may ultimately lead to dismissal. It may also be necessary to proceed with criminal charges depending on the nature of the incident.

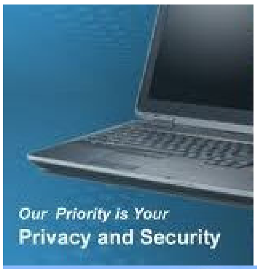
Security

Physical Security

- All staff leaving the building should ensure that that all windows are closed and the door locked and alarm set when leaving the building. The practice has a secure monitored alarm system installed.
- Rooms containing computer hardware and data should be locked when not in use and at the end of the day. A backup data drive should also be stored in the Fire safe and this secured at the end of the day.
- Copies of keys for all rooms and or filing cabinets storing confidential information must be kept in a secure location. Any sensitive data stored on the practices data network should be stored on a limited access drive.

Passwords

- Individuals using the computer network will be issued with a network username and password. Advice as to the formation of this password will be given and agreed with the IT Manager.
- Passwords must be kept confidential and must not be disclosed to anyone outside the practice.
- Laptop computers will have an appropriate boot-up password
- Users must log off the network and close down the computer when they leave the building at night, or if they leave the office to attend site or a meeting, and either the office will be left unattended, or they may not return for the evening; please do not leave your computer on thinking that some one else will log off and turn off unattended equipment.
- A password protected screen lock must be used to ensure that the system is protected when left unattended for more than an hour.
- The data store will be booted down over the weekend



Backup

For all staff using the computer network and its associated software:

- All work files should be stored on the server.
- If any work is stored temporarily on a local hard disk (for instance a laptop of home computer) it is the responsibility of the user to ensure that adequate back up takes place.
- bpArchitecture is responsible for undertaking the regular back up of the network server. The practice has a mirrored network hard drive which ensures that a duplicate copy of data is available in the event of hardware failure, this is then backed up to alternate backup discs which in turn are stored in a fire safe.

Virus Protection

- The network is loaded with approved anti-virus software and fire wall.
- Any computers owned by the practice will have appropriate virus software installed, and firewall protection implemented.
- Staff using lap-tops must ensure they load the most up-to-date virus software on their laptops as soon as it is available. This will include ensuring that virus protection is regularly updated.
- Any personal laptops brought into the office and connected to the office system, either hard wired or using wireless networking, should have virus software installed, and appropriate firewalls. .
- The practices Wireless network key will be a secure locked key. All main computers are hard wired into the office network. Where wireless network keys are provided for Ipads, Phones and other devices, it will be the responsibility of staff provided with such access to ensure that the codes are not passed on to anyone outside the practice. The practices wireless code will be changed when anyone leaves the practice, or when a potential breach/threat is identified.
- Staff must act promptly to carry out any instruction relating to virus issues as directed by the IT Team.

Hardware

- bpArchitecture have an outsourced It Department, The Principal will be responsible for all requests for hardware, and sanctioning purchase.
- The IT Team will be solely responsible for installing the equipment and all associated software.
- Maintenance of the equipment will be provided under a separate agreement with a the IT department for the payment of an annual fee.
- Visitors who need to access personal computers and network must be under the supervision of a named member of staff.

Software

- The IT Team will be responsible for installing or providing advice on installing all software.
- No software must be installed by individual staff without prior agreement.
- Permission must be sought from the IT Manager before software is added or removed. Non-authorised software packages must not be loaded on to computers.
- All software loaded on to computers should be used in accordance with

its licence agreement..

- Where personal licences are being used it is the responsibility of the licence holder to ensure that the software has been loaded legitimately, that the software is marked as having a personal licence, and that it is clear who owns the licence. It is that person's responsibility to remove the software once the requirement to use it ceases.
- When using master disks of software, staff must ensure that they are write protected.
- Any software installed must be cleared with the IT Team. Unauthorised, illegal software will be removed.

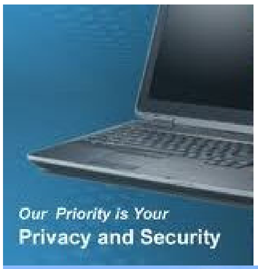
Off Site Working

- IT equipment, digital files, and paper files can only be taken off the premises with the permission of the Directors and must only be used for the business of bpArchitecture.
- Staff are responsible for ensuring the security, proper care and use of the equipment and software in their care.
- Laptops, other IT equipment and paper files must not be left unattended in public places. They should be kept in a locked boot and not be left visible when being carried in a car. Note the equipment is not and cannot be insured by the practice when left in vehicles. When viewed while travelling on public transport appropriate care and preventative measures must be taken to avoid correspondence being viewed by the public.
- Paper files and other such documentation containing client confidential information must not be left in cars, even when in a locked boot.
- Staff must ensure any confidential data taken outside the office is stored appropriately, including when working from home.
- Any software removed from the offices of bpArchitecture shall be signed in and out with the IT team.

Confidentiality

Storage of Information

- All electronic Client information must be stored on the server, in the appropriate section on the file. Generally data is stored electronically (in files that mirror the paper filing system)
- If it becomes necessary to store the data on a local hard disk on a temporary basis (e.g. CD ROM, floppy disc) it is the responsibility of the user to ensure that it is password protected and removed or destroyed as soon as possible. Only in specific circumstances can client identifiable data be used off site e.g. when working from home.
- Where any data arrives in paper format, this will be scheduled for digital scanning and stored in the appropriate electronic file. The data will be marked as scanned, Any such data will then be destroyed or kept in the appropriate project box file and stored until either destroyed or the project reaches practical completion. On rare occasions some paper files will be stored until the end of defects liability. But in most instances the data will have been scanned and stored electronically, allowing the original to be given to the Client or destroyed. This electronic policy is communicated to all Clients via the practices Terms of Business.
- Information will be retained on our files in accordance with our Client Care correspondence (agreement). The Client may retain the information following the completion of this time frame, otherwise is will be destroyed appropriately.



Use of Information

- Access to confidential data will be on a strict need-to-know basis.
- All electronic confidential data must be password protected

Disposal of Information

- Data (both electronic and paper) that is no longer required should be disposed of.
- Paper used for scrap must not include any personal data
- All confidential information held on paper that requires destroying should be shredded.
- All magnetic media for disposal should be given to the IT Team for Data Protection Compliance clearly marked in a sealed envelope 'FOR DISPOSAL'
- The IT Team will dispose of all obsolete computing hardware requiring disposal appropriately.
- All hard disks and floppy disks must be reformatted prior to disposal. It the reformatting is not possible and the disk contains confidential information then the disk will be destroyed.

Disclosure of confidential information

- No confidential information will be disclosed to anyone outside of bpArchitecture unless the recipient is using the data for bona fide project purposes, can guarantee the safe keeping of that data and guarantee to destroy the data once its use has been concluded.
- When corresponding via telephone, confidential information will only be communicated to providers of that confidential information, after verification of their identity (if the individual is not known to the caller)
- No confidential information should be left on answer phones.
- No confidential information should be transmitted via facsimile.
- No confidential information shall be transmitted via open email. If it is essential to send confidential information electronically it should be as a password protected attachment. The password should be either transmitted via telephone directly to the recipient or by letter.
- When sending confidential information by post, the envelope must be marked 'CONFIDENTIAL' and 'For addressee only'