11/12 Riverside Studios, Amethyst Road, Newcastle upon Tyne, NE4 7YL
T: 0191 213 0133 E: mail@akarchitects.net

Data Protection / Information Security Policy Statement

(Please Refer to Anthony Keith Architects Ltd FULL Quality manual BS EN ISO 9001).

Anthony Keith Architects Limited (the 'Organisation') aims to provide defect free products to its customers on time and within budget.

The Organisation operates a Quality Management System that has gained BS EN ISO 9001 : 2008 certification, including aspects specific to the provision of architectural services and associated activities.

The management is committed to:

1. Develop and improve the Quality Management System
2. Continually improve the effectiveness of the Quality Management System
3. The enhancement of customer satisfaction

AKA Data Protection Principles:

AKA is committed to complying with the data protection principles in the following terms:
As detailed in Schedule 1 to the Data Protection Act:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Use of Personal Information: AKA will not disclose information regarding our clients to third parties unless the client has first given their consent. Information collected about the client is used only for the provision of our services to the client. This information is not used for any other purpose. If you have any concerns about privacy matters please contact us at mail@akarchitects.net

Anthony Keith Architects Ltd
mail@akarchitects.net
www.akarchitects.net

REGISTERED IN ENGLAND 11/12 Riverside Studios, Amethyst Road, Newcastle upon Tyne, NE4 7YL

THINK BEFORE YOU PRINT
Royal Institute of British Architects
constructionline

11/12 Riverside Studios, Amethyst Road, Newcastle upon Tyne, NE4 7YL
T: 0191 213 0133 E: mail@akarchitects.net

AKA Information Security Principles:

AKAs Information Security Policy was drawn up in line with BS7799 requirements.

- AKA regularly review business drivers and risk posture of the organisation
- AKA regularly review the scope of the Information Security Management System (ISMS)
- AKA regularly review business critical assets & undertake a risk assessment against these

In line with the principles of BS7799 AKA regularly review and implement practices under the following areas.

1. *Business Continuity Planning*
   To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.
2. *System Access Control*
   1) To control access to information
   2) To prevent unauthorised access to information systems
   3) To ensure the protection of networked services
   4) To prevent unauthorized computer access
   5) To detect unauthorised activities.
   6) To ensure information security when using mobile computing and tele-networking facilities
3. *System Development and Maintenance*
   1) To ensure security is built into operational systems;
   2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information;
   4) To ensure IT projects and support activities are conducted in a secure manner;
   5) To maintain the security of application system software and data.
4. *Physical and Environmental Security*
   To prevent unauthorised access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.
5. *Compliance*
   1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
   2) To ensure compliance of systems with organizational security policies and standards
   3) To maximize the effectiveness of and to minimize interference to/from the system audit process
6. *Personnel Security*
   To reduce risks of human error, theft, fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; to minimise the damage from security incidents and malfunctions and learn from such incidents.
7. *Security Organisation*
   1) To manage information security within the Company;
   2) To maintain the security of organizational information processing facilities and information assets accessed by third parties.

3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer & Network Management

1) To ensure the correct and secure operation of information processing facilities;
2) To minimise the risk of systems failures;
3) To protect the integrity of software and information;
4) To maintain the integrity and availability of information processing and communication;
5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
6) To prevent damage to assets and interruptions to business activities;
7) To prevent loss, modification or misuse of information exchanged between organizations.

9. Asset Classification and Control

To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

10. Security Policy

To provide management direction and support for information security.
Within each section are the detailed statements that comprise the standard.

Reporting a security incident: If you become aware of a security-related issue, whether it relates to a problem with a computer in your department or a system elsewhere, please report it to The Computer management team. Even if you resolve the matter yourself, it is helpful for us to gather statistics on the number and nature of incidents. We will, if you wish, preserve anonymity.

Vulnerabilities: Microsoft: Microsoft does not permit the mirroring or redistribution of its bulletins. Instead, consult the Microsoft TechNet site at http://www.microsoft.com/technet/security/current.asp. (The site has been enhanced to allow you to identify the patches relevant to your operating system and service pack level.)

Viruses: AKA has site licences for a number of anti-virus products.
Unfortunately, however dutifully you keep your anti-virus software up-to-date, you may still fall foul of a new, hitherto unknown virus. Most a/v packages look for particular patterns, and will not identify a new virus until they have been taught the new pattern. What can you do? Here are some suggestions for staying virus-free:

1. Don't open attachments people send you without knowing what they contain.
2. Staff are forbidden to download software, games, screensavers from the Internet, or even from a friend's computer. Be especially wary at Christmas when more of these things seem to be in circulation!

This Data Protection / Information Security Policy is regularly reviewed in order to ensure its continuing suitability.

Copies of the Data Protection / Information Security Policy are made available to all members of staff. Copies of the minutes of Management Reviews, or extracts thereof, are provided to individual members of staff in accordance with their role and responsibilities as a means of communicating the effectiveness of the Quality Management System.

11/12 Riverside Studios, Amethyst Road, Newcastle upon Tyne, NE4 7YL
T: 0191 213 0133 E: mail@akarchitects.net

This Policy is communicated to all employees, suppliers and sub-contractors and is made available to the public.

Daniel Cogdon:  Date: 3rd January 2018

Director

Anthony Keith Architects Ltd
mail@akarchitects.net
www.akarchitects.net

REGISTERED IN ENGLAND 11/12 Riverside Studios, Amethyst Road, Newcastle upon Tyne, NE4 7YL

THINK BEFORE YOU PRINT

Royal Institute of British Architects

constructionline