DATA PROTECTION POLICY

Version Number	Purpose/Change	Author	Date
1.0	First version	Asb law	14/2/2013
1.0	Reviewed	Sue Burchett	2/8/16

1. POLICY STATEMENT

1.1. Everyone has rights with regard to how their personal information is handled. Albion in the Community ("AITC") during the course of its activities will collect, store and process personal information about its staff and other users, and AITC recognises the need to treat it in an appropriate and lawful manner.

1.2. The types of information that AITC may be required to handle include details of current, past and prospective employees, suppliers, funders, customers, players, students, apprentices, and others that AITC communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 ("the Act") and other regulations. The Act imposes restrictions on how AITC may use that information.

1.3. This policy does not form part of any employee's contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by AITC from time to time. Any failure to follow the policy will be taken seriously and may result in disciplinary action.

2. STATUS OF THE POLICY

2.1. This policy sets out AITC's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2. The Data Protection Compliance Officer is responsible for ensuring compliance with the Act and with this policy. That post is held by Sue Burchett, extension 2031, dataprotection@albioninthecommunity.co.uk. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Compliance Officer.

2.3. If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter initially with your line manager. If the matter is not resolved, it should be raised as a formal grievance or complaint. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Compliance Officer.

3. DEFINITION OF DATA PROTECTION TERMS

3.1. **"Data"** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2. **"Data subjects"** for the purpose of this policy include all living individuals about whom AITC hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3. **"Personal data"** means data relating to a living individual who can be identified from that data (or from that data and other information in AITC's possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4. **"Data controllers"** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. AITC is the data controller of all personal data used in AITC's business.

3.5. **"Data users"** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following AITC's data protection and security policies at all times.

3.6. **"Data processors"** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on AITC's behalf.

3.7. **"Processing"** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8. **"Sensitive personal data"** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

4.1.1. Processed fairly and lawfully.

4.1.2. Processed for limited purposes and in an appropriate way.

4.1.3. Adequate, relevant and not excessive for the purpose.

4.1.4. Accurate.

4.1.5. Not kept longer than necessary for the purpose.

4.1.6. Processed in line with data subjects' rights.

4.1.7. Secure.

4.1.8. Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1. The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case Albion in the Community), who the data controller's representative is (in this case the Data Protection Compliance Officer), the purpose for which the data is to be processed by us and confirmation of whether the data is disclosed or transferred to any other third parties for processing. AITC shall notify data subjects of this through the privacy policy / information provided to the data subject at the time the data is collected by AITC.

5.2. For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, the data subject's explicit consent to the processing of such data will generally be required, for example, where we ask for information which relates to an individual who may have a disability and AITC needs that information in order to assess and assist with access for that individual to the premises, eg, for courses.

6. PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. As mentioned above, this will generally be achieved through AITC's privacy policy and/or through information that is provided to individuals at the time the personal data is collected from them, even if this is over the telephone. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from AITC's systems when it is no longer required. For guidance, Appendix 1 details how long certain data is to be kept before being destroyed.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

10.1.1. Request access to any data held about them by a data controller.

10.1.2. Prevent the processing of their data for direct-marketing purposes.

10.1.3. Ask to have inaccurate data amended.

10.1.4. Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. DATA SECURITY

11.1. AITC must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2. The Act requires AITC to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

11.3.1. **"Confidentiality"** means that only people who are authorised to use the data can access it.

11.3.2. **"Integrity"** means that personal data should be accurate and suitable for the purpose for which it is processed.

11.3.3. **"Availability"** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on AITC's central computer system instead of individual PCs.

11.4. Security procedures include:

11.4.1. **"Entry controls"** Any stranger seen in entry-controlled areas should be reported.

11.4.2. **"Secure lockable desks and cupboards"** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

11.4.3. **"Methods of disposal"** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

11.4.4. **"Equipment"** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

12. DEALING WITH SUBJECT ACCESS REQUESTS

12.1. Staff and other users of AITC (known as a data subject) have the right to access any personal data that is being kept about them either on a computer or in certain paper files.

12.2. A formal request from a data subject for information that AITC holds about them must be made in writing. AITC may make a reasonable charge of up to £10 payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to the Data Protection Compliance Officer immediately.

12.3. AITC aims to comply with requests for access to personal data as quickly as possible, but is required to comply with requests within 40 days from receipt of the request or from the receipt of the information necessary to enable compliance with the request, whichever is later.

13. PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by AITC. In particular they should:

13.1.1. Check the caller's identity to make sure that information is only given to a person who is entitled to it.

13.1.2. Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

13.1.3. Refer to their line manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

14. TELECOMMUNICATIONS AND IT INFRASTRUCTURE

14.1. Computer accounts are the property of AITC and are designed to assist in the performance of the work of employees. There should, therefore, be no expectation of privacy in any stored work or messages sent or received whether of a business or of a personal nature.

14.2. When sending emails or other electronic messages on AITC's system or using AITC's equipment, the sender is consenting to the processing of any personal data contained in that email or other electronic message and is explicitly consenting to the processing of any sensitive personal data contained in that email or other electronic message. If individuals do not wish AITC to process such data, they should communicate it by other means.

14.3. AITC has the right to monitor any and all aspects of its telephone, computer and electronic systems, and to monitor, intercept and/or record any communications made or received by employees, including telephones, email, internet or other electronic communications.

14.4. Further information is available in AITC's IT, Internet Use & Social Media policy.

15. CONCLUSION

Compliance with the Act is the responsibility of all staff of AITC. Any deliberate breach of this data protection policy may lead to disciplinary action being taken or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with your line manager.

16. REVIEW

This policy will be reviewed on an annual basis.

Appendix 1 RETENTION PERIODS

Type of Data	Retention Period	Reason
Personnel Files; training records; notes of grievance and disciplinary hearings	6 years from the end of employment	Provision of references and limitation period for litigation
Staff Application forms; interview notes	6 months from the date of the interviews	Limitation period for litigation
Facts relating to redundancies (less than 20 redundancies)	3 years from the date of redundancies	Limitation period for litigation
Facts relating to redundancies (20 or more redundancies)	12 years from the date of redundancies	Limitation period for litigation
Income Tax and NI returns; correspondence with Tax Office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	At least 3 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	At least 3 years after the end of the financial year to which the records relate	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years from the last date of employment	Taxes Management Act 1970
Accident Books, records and reports of accidents	3 years after the date of the last entry	RIDDOR 1995
Health Records	During Employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is concerned with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances hazardous to health	40 years	COSHH 1999
Student and Apprentice Records including academic achievements, and conduct	At least 6 years from the last day of the course. 10 years with the consent of the student for personal and academic references.	Limitation period for negligence