As-Suffa Trust

Data Protection Policy

Last Review Date: April 2018

Next Review Date: April 2020

1.0 Introduction

1.1 Purpose of Policy

1.1.1 As-Suffa Trust is committed to protecting the rights and privacy of individuals.

1.1.2 As-Suffa Trust needs to collect and use certain types of Personal Data (this includes sensitive personal data). This personal information should be collected and dealt with accordance to the Data Protection Act 1998.

1.1.3 The purpose of this policy is to ensure that As-Suffa Trust:

1.1.3.1 Complies with the law in respect of the data it holds and it processes of individuals

1.1.3.2 Sets out procedures for protecting and handling personal data

1.1.3.3 Maintains the confidentiality of personal data

1.1.3.4 Protects the organisation from the consequences of any breaches

1.2 Scope of Policy

1.2.1 This policy applies to personal data (data which relates to a living individual who can be identified) handled and processed by As-Suffa Trust.

1.2.2 This policy applies to the following premises:

1.2.2.1 As-Suffa Institute, 156 High Street, Aston, Birmingham B6 4UX

1.2.2.2 As-Suffa Institute (*Charity Registered Address*), 25 Park Lane, Aston, Birmingham B6 5DA

1.2.2.3 Projects and activities co-ordinated by As-Suffa Outreach, operating at various locations across the UK. These are referred to as ***operational sites***. These sites are not necessarily owned by As-Suffa Trust but may be booked, hired, offered to, or rented by As-Suffa Trust.

1.2.2.4 Projects and activities that take place in third party venues and premises are referred to as ***activity sites***.

1.2.3 This policy applies to employees, volunteers, contractors and organisations we work with.

1.2.4 This policy does not apply to third party Data Controllers such as online website plugins, online applications, and other online systems where personal data is not collected, handled or processed by As-Suffa Trust.

1.3 Policy Statement

1.3.1 As-Suffa Trust is committed to act upon the principles set by the DPA (Data Protection Act). Personal information should:

1.3.1.1 be processed fairly and lawfully;
1.3.1.2 not be used for a purpose for which it was not collected;
1.3.1.3 be adequate, relevant and not excessive for the purpose;
1.3.1.4 be accurate and up-to-date;
1.3.1.5 not be kept longer than necessary;
1.3.1.6 be processed in accordance with the data subject's rights;
1.3.1.7 be kept secure and protected from unauthorised processing, loss or destruction; and
1.3.1.8 be transferred only to those countries outside the European Economic Area that provide adequate protection for personal information

1.3.2 In order to meet the requirements of the principles set by DPA, As-Suffa Trust will:

1.3.2.1 observe conditions regarding the fair collection and use of information;
1.3.2.2 meet its legal obligations to specify the purposes for which information is used;
1.3.2.3 collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
1.3.2.4 ensure the quality of the information used;
1.3.2.5 hold personal information on for as long as it is necessary for the relevant purpose;
1.3.2.6 ensure that the rights of people about whom information is held can be fully exercised under the Act (these include: the right to be informed that processing is being undertaken; the data subject's right of access to their personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information);
1.3.2.7 take appropriate technical and organisational security measures to safeguard personal information; and
1.3.2.8 ensure that personal information is not transferred outside the EEA without suitable safeguards

2.0 Responsibilities

2.1 The Board of Trustees

Responsibilities of the Board are:

2.1.1 overall responsibility for the data protection within the organisation;
2.1.2 ensure As-Suffa are compliant to relevant law and regulations in regards to data protection;
2.1.3 ensure procedures are in place to handle, process and manage personal data safely and securely;
2.1.4 make the senior management aware about this policy and its implementation;
2.1.5 informing the senior management of any changes, amendments, implementation and procedures under this policy;
2.1.6 approving unusual or controversial disclosures of personal data; and
2.1.7 appoint a delegated staff member to administer and manage Data protection throughout the organisation
2.1.8 The **responsible person** to overlook Data Protection for the organisation is Shaykh Zahir Mahmood.

2.2 Senior Management (SM)

The senior management consists of:

- Line Managers
- Administrators
- Project Managers
- Maktab Head
- Maktab Deputy Head
- Course Director
- Event Coordinators
- Volunteer Leads
- Facilities Manager

Responsibilities of members of the senior management who are entrusted with handling or processing personal data, but not limited to, are:

2.2.1 to be aware of the As-Suffa Data Protection Policy;
2.2.2 to be aware of the requirements of the DPA and how the rules apply to them;
2.2.3 to ensure, if entrusted, to implement the procedures of this policy;
2.2.4 ensure that policies within this document are not breached;
2.2.5 ensure Data Protection induction and training takes place for new employees, volunteers or contractors, where appropriate;
2.2.6 ensure staff, volunteers and contractors are aware and kept up-to-date with Data Protection Law;

2.2.7 respect confidential information in their possession and maintain information security; and
2.2.8 to operate within UK Data Protection regulation

2.3 Delegated Staff Member

Responsibilities of the delegated member of staff are:

2.3.1 brief the Board of Trustees on Data Protection responsibilities;
2.3.2 review alongside with the Board, Data Protection and related policies;
2.3.3 advise other staff in Data Protection issues;
2.3.4 handle and liaise with the responsible person in regards to 'Subject Access Requests';
2.3.5 ensure IT systems are secure and able to handle personal data efficiently;
2.3.6 ensure everyone managing and handling personal information understands that they are responsible for following good data protection practice;
2.3.7 ensure everyone managing and handling personal information is appropriately trained;
2.3.8 ensure queries about handling personal information are promptly and courteously dealt with, and clear information is available to all relevant staff and volunteers; and
2.3.9 review, assess, and evaluate its procedures, methods and performance in relation to handling personal information
2.3.10 The delegated staff member is

2.4 Staff/Volunteers

Responsibilities of staff (includes contractors)/volunteers who are entrusted with handling or processing personal data are:

2.4.1 to be aware of the As-Suffa Data Protection Policy;
2.4.2 to be aware of the requirements of the DPA and how the rules apply to them;
2.4.3 complete Data Protection induction and any necessary training;
2.4.4 to ensure, if entrusted, to implement the procedures of this policy;
2.4.5 ensure that policies within this document are not breached;
2.4.6 respect confidential information in their possession and maintain information security and
2.4.7 to operate within UK Data Protection regulation

3.0 Key Definitions

3.1 It is important for all staff, volunteers and contractors to recognise and understand key definitions referred to Data Protection. Understanding these definitions will reduce the risk of breaching this policy and Data Protection law. Further information is provided (see Appendix Section).

3.2 Data

This means information which:

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
b) is recorded with the intention that it should be processed by means of such equipment,
c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

3.3 Personal Data

This means data which relates to a living individual who can be identified:

a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

3.4 Sensitive Data

This means personal data consisting of information as to:

a) the racial or ethnic origin of the data subject,
b) his political opinions,
c) his religious beliefs or other beliefs of a similar nature,
d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
e) his/her physical or mental health or condition,
f) his/her sexual life,
g) the commission or alleged commission by him/her of any offence, or
h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings

3.5 Processing

This means in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

a) organisation, adaptation or alteration of the information or data,
b) retrieval, consultation or use of the information or data,
c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data

4.0 Procedures

4.1 Principles

In order to understand why these procedures are in place the following explanations of the principles should be read and understood:

4.1.1 Principle 1 (Fair and Lawful)

4.1.1.1 Before collecting any new personal data (via paper form or online), it should be transparent on how an individual's information will be used and that they are aware we will be processing their data. This should be done by providing a reason via on paper form or online. See As-Suffa Trust Privacy Policy/Notice for more details.

4.1.1.2 Personal data should not be obtained unlawfully and without the individual's consent.

4.1.1.3 For using personal data for a new purpose, it should be thought as to whether the individual is likely to reasonably expect As-Suffa Trust to use their personal data. If not sure, then intentions should be explained and a 'opt out' option should be made available to the individual.

4.1.1.4 This also includes how we may need to disclose personal data.

4.1.2 Principle 2 (Conditions of Processing)

4.1.2.1 At least one of the following conditions must be met whenever personal data is processed:

4.1.2.1.1 The individual whom the personal data is about has consented to the processing;

4.1.2.1.2 the processing is necessary in relation to a contract which the individual has entered into; or

4.1.2.1.3 because the individual has asked for something to be done so they can enter into a contract;

4.1.2.1.4 the processing is necessary because of a legal obligation that applies to us (except an obligation imposed by a contract);

4.1.2.1.5 the processing is necessary to protect the individual's "vital interests" (this condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's, A&E department treating them or after a serious road accident);

4.1.2.1.6 the processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions and

4.1.2.1.6.1 the processing is in accordance with the "legitimate interests" condition

4.1.3 Principle 3 (Purpose)

4.1.3.1 Before collecting personal data via paper form or online, we must:

4.1.3.1.1 be clear from the outset about why we are collecting personal data and what we intend to do with it;

4.1.3.1.2 comply with the DPA's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;

4.1.3.1.3 comply with what the DPA says about notifying the Information Commissioner; and

4.1.3.1.4 ensure that if we wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair

4.1.4 Principle 4 (Adequacy)

4.1.4.1 When collecting personal data, we must ensure:

4.1.4.1.1 personal data about an individual is sufficient for the purpose we are holding it for in relation to that individual; and

4.1.4.1.2 we do not hold more information than we need for that purpose

4.1.5 Principle 5 (Accuracy)

4.1.5.1 Personal data that we have stored on paper file or electronic, we should ensure:

4.1.5.1.1 to take reasonable steps to ensure the accuracy of any personal data we obtain;
4.1.5.1.2 that the source of any personal data is clear;
4.1.5.1.3 to carefully consider any challenges to the accuracy of information; and
4.1.5.1.4 to consider whether it is necessary to update the information

4.1.5.2 Principle 6 (Retention)

4.1.5.2.1 Personal data processed for any purpose should not be kept for longer than it is necessary for that purpose of those purposes, we should ensure to:

4.1.5.2.1.1 review the length of time we keep personal data;
4.1.5.2.1.2 consider the purpose or purposes we hold the information in deciding whether (and for how long) to retain it;
4.1.5.2.1.3 securely delete information that is no longer needed for this purpose or these purposes; and
4.1.5.2.1.4 update, archive or securely delete information if it goes out of date

4.1.5.3 Principle 6 (Rights)

4.1.5.3.1 Individuals have the right to be informed of the personal data we hold about them, we should ensure that individuals who we hold personal data have:

4.1.5.3.1.1 a right of access to a copy of the information comprised in their personal data;
4.1.5.3.1.2 a right to object to processing that is likely to cause or is causing damage or distress;
4.1.5.3.1.3 a right to prevent processing for direct marketing;
4.1.5.3.1.4 a right to object to decisions being taken by automated means;
4.1.5.3.1.5 a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
4.1.5.3.1.6 a right to claim compensation for damages caused by a breach of the DPA

4.1.5.4 Principle 7 (Security)

4.1.5.4.1 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to, personal data.

4.1.5.5 Principle 8 (International)

4.1.5.5.1 Personal data should not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

4.2 Procedures

4.3 The procedures for the collection and handling of personal information apply to all personal information created or collected by As-Suffa Trust and its staff and volunteers in the course of their required work.

4.4 The information will include, but not limited to,:

4.4.1 the names and other detail of employees, contractors, volunteers, students and service users;
4.4.2 the names and other details of those who correspond with us or provide details during telephone calls;
4.4.3 information about contractors and suppliers of goods and services;
4.4.4 information held by members of SM about their staff or volunteers, such as performance management information etc.;
4.4.5 paper and electronic documents, spreadsheets and databases which contain personal details such as names, addresses, data of birth and other sensitive data; and
4.4.6 emails, where either the individual sending or receiving is identifiable or the contents refer to identifiable individuals

4.5 The following procedures should be followed in order to meet the requirements of the DPA principles mentioned above:

4.5.1 Data Collection

4.5.1.1 Before any personal data is collected, the As-Suffa 'Data Protection Data Process Form' must be completed. When filling out the form, this Policy should be considered as guidance.
4.5.1.2 The completed form should be handed to the Administration team who will then process the form and check the request is compliant with DPA.

4.5.2 Data Processing

4.5.2.1 Personal data that is collected on paper form should be processed accordingly to electronic form where appropriate.

4.5.2.2 Personal data should only be processed by authorised staff members.

4.5.2.3 Non-authorised staff members should not handle or process personal data.

4.5.2.4 Personal data that is processed electronically must be processed on authorised As-Suffa Trust IT computers. Personal computers, personal laptops or any personal electronic devices should not be used to process personal data unless certain personal devices have been checked and authorised by the senior management.

4.5.3 Data Storage

4.5.3.1 All paper forms that contain personal data should be safely stored in a secure filing cabinet depending on which premises the filing cabinet is located.

4.5.3.2 Personal data of individuals should be stored in the correct filing systems, categories and sections.

4.5.3.3 All filing cabinets that store personal data should be secure and locked at all times.

4.5.3.4 Only authorised staff members can access the filing cabinets.

4.5.3.5 Personal data that has been processed electronically should be stored on the secure I.T systems used by the organisation.

5.0 Breaches/Risks

5.1 Any breaches of this policy can result to disciplinary action (see As-Suffa Trust Disciplinary Policy). The following breaches/risks can put As-Suffa Trust, staff and volunteers into consequences with the law. All staff and volunteers should bear this to mind:

5.1.1 Breach of confidentiality

5.1.1.1 This is where personal or sensitive information has been given out inappropriately by a member of staff or volunteer

5.1.2 Beach of data security

5.1.2.1 Unauthorised individuals have access to personal data

5.1.3 Data consistency

5.1.3.1 Personal data no up-to-date

5.1.3.2 Inaccurate data

5.1.4 Data responsibility

5.1.4.1 Insufficient clarity on how personal data will be used

5.1.4.2 Insufficient procedures in place to handle and keep personal data secure

6.0 Data Recording and Storage

6.1 Accuracy

6.1.1 As-Suffa will be using databases to hold basic information about employees, contractors, volunteers, students and service users if applicable.

6.1.2 IT systems will be used, where possible, to encourage and facilitate the entry of accurate data.

6.1.3 Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.

6.1.4 Effective procedures should be in place so that all relevant systems are updated when information about any individual changes.

6.1.5 Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

6.2 Retention Periods

6.2.1 As-Suffa will establish retention periods for at least the following categories of personal data:

6.2.1.1 Employees

6.2.1.2 Contractors

6.2.1.3 Volunteers

6.2.1.4 Students

6.2.1.5 Service Users

6.3 Data Storage

6.3.1 Personal data on paper form should be stored securely in lockable filing cabinets/cabinets.

6.3.2 Processed personal data electronically must be stored on only As-Suffa PC's, storage devices or secure online systems.

6.3.3 Personal data should not be stored on personal computers/laptops or other electronic devices.

6.4 Authorised Access

6.4.1 Only authorised staff or volunteers can handle and process personal data.

6.4.2 Authorised individuals should complete the Confidentiality Statement Form.

6.5 Archiving

6.5.1 Any archived data, which does not contain personal data, should be stored securely off site.

7.0 Keeping Personal Data Secure

7.1 Physical Storage

7.1.1 All filing cabinets/cabinets should be lockable with a key. The key should be stored in a secure holding. Only authorised individuals should access when required to.

7.1.2 Rooms which the filing cabinets/cabinets are located in should be lockable. Only authorised individuals should access when required to.

7.1.3 Keys to the filing cabinet/cabinets should be kept secure in a lockable key holder/cabinet. Only the authorised individuals should have access to the key holder/cabinet.

7.1.4 Paper copies of personal data should not be left around where anyone else can access them.

7.2 IT Systems

7.2.1 All personal data processed or stored on computers should be on authorised As-Suffa Trust computers and electronic devices. Personal computers, laptops or other electronic devices should not be used unless authorised by a member of the SM whilst ensuring appropriate measures have been taken to use personal equipment.

7.2.2 All As-Suffa Trust PC's laptops and other relevant devices should have business industry level firewall and anti-virus protection. The protection software should be regularly updated and regular scans should be initiated.

7.2.3 All PC's, laptops and other relevant electronic devices should be password protected and issued by a competent staff member who overlooks the IT in As-Suffa Trust.

7.2.4 Passwords should not be shared with colleagues or family members.

7.2.5 Passwords should not be written down or physically stored by staff or volunteers.

7.2.6 Computers should not be left unattended without locking the computer. This should also be done if an individual is close enough to see the information on the screen.

7.2.7 Particular care should be taken to ensure security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

7.2.8 This policy also applies to staff and volunteers who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and volunteers should take particular care when processing personal data at home or in other locations outside As-Suffa Premises.

8.0 Rights of Access to Data

8.1 Individuals ,whom As-Suffa Trust holds personal data about, have the right to access any personal data which are held by As-Suffa Trust in electronic format and paper form which form part of a relevant filing system. This includes the right to inspect confidential personal references received by As-Suffa Trust about that person.

8.2 Any individual who wishes to exercise this right should apply in writing to the As-Suffa Administration team. As-Suffa Trust reserves the right to charge a fee for data subject access request (currently £10.00).

8.3 An As-Suffa Subject Access Request Form will have to be filled in and handed to the Administration team.

8.4 Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

9.0 Disclosure of Data

9.1 As-Suffa Trust must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and volunteers should exercise caution when asked to disclose personal data held on another individual to a third party.

9.2 In some circumstances, some data may be disclosed, such as disclosing a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regrading a non-work related matter.

9.3 Staff and volunteers should bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of As-Suffa Trust business.

9.4 Best practice would be to take the contact details of the person making the enquiry and pass them onto the member of As-Suffa Trust concerned.

9.5 This policy determines that personal data may be correctly disclosed where one of the following condition apply:

9.5.1 the individual has given their consent (e.g. employee, volunteer or student has consented to As-Suffa Trust corresponding with a named third party);

9.5.2 where the disclosure is in the correct interests of the organisation (e.g. disclosure to staff - personal information can be disclosed to other As-Suffa Trust employees if it is clear that those members of staff require the information to enable them to perform their jobs);

9.5.3 where As-Suffa Trust is legally obliged to disclose the data (e.g. ethnic minority and disability monitoring etc.); and

9.5.4 where disclosure of data is required for the performance of a contract (e.g. partnership with other organisations)

9.6 The DPA permits certain disclosures without consent so long as the information is requested for one or more of the following purposes (supported by appropriate paperwork/evidence):

9.6.1 to safeguard national security;

9.6.2 prevention or detection of crime including the apprehension or prosecution of offenders;

9.6.3 assessment or collection of tax duty;

9.6.4 discharge of regulatory functions (includes health, safety and welfare of persons at work);

9.6.5 to prevent serious harm to a third party; and

9.6.6 to protect the vital interests of the individual, this refers to life and death situations

10.0 Retention and Disposal of Data

10.1 As-Suffa Trust discourages the retention of personal data for longer than they are required.

10.2 Considerable amounts of data are collected on current employees, contractors, volunteers, students and various service users. Once anyone of these individuals leave As-Suffa Trust or do not receive services over a period of time, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others, such as students.

11.0 Direct Marketing

11.1 Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals should be provided with the opportunity to object to the use of their data for direct marketing purposes e.g. an opt-out box on a form or unsubscribe link on emails.

12.0 Use of CCTV

12.1 For reasons of personal security and to protect As-Suffa Trust premises and the property of employees, contractors, volunteers and service users, CCTV is in operation in certain locations within As-Suffa premises.

12.2 More detailed policies and procedures can be found in the As-Suffa CCTV Policy.

13.0 Useful Contacts

13.1 Administration Team

- 13.1.1 Location: Comms Room Office
- 13.1.2 Email: admin@as-suffa.org
- 13.1.3 Contact: 0121 285 2777 extension 1000

13.2 Delegated Staff responsible for Data Protection within As-Suffa Trust

- 13.2.1 Name: Yassar Taj
- 13.2.2 Email: yassartaj@as-suffa.org
- 13.2.3 Contact: 0121 285 2777(extension 1000)/07804 636 290

13.3 Responsible Person for overall Data Protection within As-Suffa Trust

- 13.3.1 Name: Shaykh Zahir Mahmood
- 13.3.2 Email: zahir@as-suffa.org
- 13.3.3 Contact: 0121 285 2777 extension 1003

14.0 Appendix

14.1 The Data Protection Act

The Data Protection Act controls how your personal information is used by organisations, businesses or the government.

Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully;
- used for limited, specifically stated purposes;
- used in a way that is adequate, relevant and not excessive;
- accurate;
- kept for no longer than is absolutely necessary;
- handled according to people's data protection rights;
- kept safe and secure; and
- not transferred outside the European Economic Area without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background;
- political opinions;
- religious beliefs;
- health;
- sexual health; and
- criminal records

14.2 8 Principles of Data Protection

First principle - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met and in the case of sensitive personal data, at least one of the conditions set out in Schedule 3 or either of the two Statutory Instruments below is met.

Second principle - 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.

Third principle - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth principle - Personal data shall be accurate and, where necessary, kept up to date.

Fifth principle - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Sixth principle - Personal data shall be processed in accordance with the rights of data subjects under this Act.

Seventh principle - 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.

Eighth principle - 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.

14.3 Definitions (Data Protection Act 1998)

Personal Data	Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.
Sensitive Data	Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.
Data Controller	Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.
Data Subject	Any living individual who is the subject of personal data held by an organisation.
Processing	Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data.
Third Party	Any individual/organisation other than the data subject, the data controller (As-Suffa Trust) or its agents.
Relevant Filing System	Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

As-Suffa Trust Data Protection Policy Agreement

I have read and understood the As-Suffa Data Protection Policy. I accept and agree to abide by this Policy which can be subject to change on a yearly basis or as when required.

Full Name:	
Signature:	
Date:	

The Board of Trustees have accepted and intended to implement this version of the As-Suffa Data Protection Policy.

Trustee Signatures: Shaykh Zahir Mahmood (Chair) Arif Mahmood (Secretary) Tahir Mahmood (Treasurer)	
Date:	