THE ARNEWOOD SCHOOL

11 – 19 Academy

"Working Together – Shaping Tomorrow"

ARN/0015

DATA PROTECTION ACT POLICY STATEMENT

POLICIES AND PROCEDURES PROFORMA

Subject and Version of Document:	Data Protection Act
Author:	Head of School/HR Advisor
Persons/Committees etc consulted whilst document in draft:	Governing Body
Date agreed:	
Date of next review/update and by whom:	April 2017
By whom agreed:	Governing Body
Copy obtainable from and/or distribution:	PA to Head Teacher
Date document issued and placed on website:	
Responsibility for dissemination to new staff:	Line Manager
Principal Target Audience:	All staff

Amendments Summary:

Amend. No.	Issued	Page	Subject
1	Nov 2011		New front cover and proforma
2	Feb 2012		Page 3 – Point 1.9 – password criteria change i.e. 9 characters
3	May 2015		Document rewritten

DATA PROTECTION ACT
POLICY STATEMENT

1.0 Policy Statement

1.1 The Arnewood School is required to retain certain information about its employees, learners and other users in order to facilitate the monitoring of performance, achievements, and health and safety and as part of our safeguarding procedures. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information stored in files (either paper based or electronically including on a computer including e-mail, internet, intranet or portable storage device) covered by the data protection legislation must be collected and used fairly, stored and disposed of safely, and not disclosed to any other person unlawfully. To do this, the School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).

1.2 In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not to be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

1.3 The school and all staff or others who process or use any personal information must ensure the school has developed the Data Protection policy.

1.4 There is stronger legal protection for information that falls under any of the 9 protected characteristics of the equality and diversity guidelines and legislation.

1.5 The 9 protected characteristics are;

- Age
- Disability
- Gender reassignment
- Marriage and civil partnership
- Pregnancy and maternity
- Race
- Religion and belief
- Sex
- Sexual orientation

2.0 Scope

2.1 This policy applies to all members of the school community (staff (including agency workers), governors, learners, contractors/suppliers and members of the public).

2.2 This policy does not form part of the formal staff contract of employment nor of the student home school agreement with the school, but it is a condition of both contracts that school policies must be adhered to. A failure to follow the policy may result in disciplinary proceedings.

2.3 Any members of staff or learners who consider that the policy has not been followed in respect of personal data about themselves or about other data subjects should raise the matter with the designated data controller* initially (learners may wish to do this through their lecturer or course tutor). If the matter is not resolved it should be raised as a formal complaint or grievance or through the school's Public Interest Disclosure (Whistle blowing) Procedure where appropriate.

3.0 Notification of Data Held and Processed

3.1 All staff, learners and other data subjects are entitled to

- know what information the school holds and processes about them and why
- know how to gain access to it
- know how to keep it up to date
- know what the School is doing to comply with its obligations under the 1998 Act

3.2 The school will advise staff and learners and other relevant data subjects about the types of data the school holds and processes about them, and the reasons for which it is processed. This will be notified via application/enrolment or other documentation.

4.0 Legislation

- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Education Act 2002

5.0 Responsibilities

5.1 All school staff have responsibility for

i. Checking that information they provide to the school in connection with their employment is accurate and up to date.
ii. Informing the school of changes to information which they have provided, e.g. Change of address.
iii. Checking the information that the school will send to them from time to time, which gives details of information kept and processed about them.
iv. Informing the school of any errors or changes. The school cannot be held responsible for any errors which staff members have had the opportunity to correct.

5.2 If and when, as part of their responsibilities, staff collect information about other people, (i.e. about learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances) they need to follow the data collection principles and guidelines for staff in Appendix 3.

5.3 The Data Controller and the Designated Data Controller. The School as a Body Corporate is the Data Controller under the Act and the Board of Governors is therefore ultimately responsible for ensuring implementation of the Act. However, the designated data controller will deal with day to day matters.

5.4 **The designated Senior Leader is the designated data controller.**

6.0 Data Security

6.1 Information Security

6.2 All staff have responsibility for ensuring that:

- Data has only been removed with the permission of the designated Data Controller
- Any personal data which they hold is stored and disposed of securely.

- Personal information is not disclosed orally, in writing, accidentally, or otherwise to any unauthorised third party
- Breaches of data security, including their own, are reported to the Data Controller and SLT.

N.B. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

6.3 Personal information should be stored securely, usually this means

- in a locked office, or
- in a locked filing cabinet, or
- in a locked drawer, or
- if it is computerised, be adequately password protected, or
- if it is kept on portable storage (i.e. USB, laptop etc..) be encrypted and itself kept securely

6.4 Unauthorised Access

6.4.1 Any member of staff or student who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party may be disciplined in accordance with school procedures.

6.5 Student/Parent/Carers Obligations

6.5.1 Student/Parents/Carers must ensure that all personal data provided to the school is accurate and up to date. They must ensure that changes of address, etc, are notified to the school.

7.0 Rights of Access to Information

7.1 Staff, learners and other data subjects have the right of access to any personal data that are being kept about them either on computer or in certain other files. Any person who wishes to exercise this right should complete the School "Request for Access to Information Form" (Appendix 1) and give it to the designated data controller.

7.2 The school will normally make a charge of £20 on each occasion that access is granted, although it has discretion to waive this charge for good reason at the discretion of the Data Controller.

7.3 The school aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

N.B There are some situations when organisations are allowed to withhold information, e.g. if the information's about:

- the prevention, detection or investigation of a crime
- national security or the armed forces
- the assessment or collection of tax
- judicial or ministerial appointments
- an organisation does not have to say why they are withholding information.

8.0 Requests for Access by 3rd Parties

8.1 The Data Protection Act includes a number of non-disclosure exemptions, these include:

- Prevention and detection of crime, capture or persecution of offenders, assessment or collection of tax or duties.

- Regulatory activity, for example, protecting members of the public from dishonesty, malpractice, incompetence of improper conduct
- Disclosure required by law, such as an order of court.
- In connection with legal proceedings, obtaining legal advice and defending legal rights

8.2 Where a 3rd party, such as the Police, makes a request for data under one of the above exemptions the "Data Access Request Form" (Appendix 1) should be completed and returned to the Data Controller.

8.3 No data should be released until the request form has been appropriately processed and release agreed by either the Data Controller, or a member of Senior Leadership Team.

9.0 Public Domain

9.1 Information that is already in the public domain is exempt from the 1998 Act. For further details please see the Publication Scheme.

- The school's internal phone list will not be a public document.
- The school's first aider list will not be in a public document.

9.2 Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data controller.

10.0 Subject Consent

10.1 In many cases, the school can only process personal data with the consent of the individual. In some cases, if the data are sensitive, express consent must be obtained. Data is considered sensitive if it is about an individual's race; political opinions; religious beliefs; trade union membership; health; sex life or criminal record.

10.2 Agreement to the school processing some specified classes of personal data is a condition of acceptance of a student into any class, and a condition of employment for staff. This includes information about previous convictions.

10.3 As most jobs within the school will bring the applicants into contact with children, including young people between the ages of 14 and 17, the school has a duty under the Education Act 2002 and other enactments to ensure that staff are suitable for the job, and learners for the courses offered. The school also has a duty of care to all staff and learners and must therefore make sure those employees, and those who use the school facilities, do not pose a threat or danger to other users.

10.4 The school will also ask for information about particular health needs, such as allergies to particular forms of medication or any conditions such as asthma or diabetes. The school will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

10.5 Therefore, all prospective staff and learners will be asked to sign a Data Collective (Consent to Process) form appendix 2, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

11.0 Processing Sensitive Information

11.1 Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the School is a safe place for everyone, or to operate other school policies, such as the sick pay policy or equality and diversity policy.

11.2 As this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the school to do this.

11.3 Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

12.0 Examination Marks

Learners will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The school may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned. The school may withhold unmoderated grade as these are subject to exam based processes.

13.0 Retention of Data

13.1 The school will retain records in line with Hampshire County Council's School Records Retention Schedule.

13.2 A full list of information with retention times is available from the designated Data Controller.

APPENDIX 1

THE ARNEWOOD SCHOOL

CONSENT TO PROCESS DATA FORM

I give my consent to The Arnewood School recording and processing such information about me as may be necessary for the proper administration of the employment relationship, both during and after employment, provided that proper regard is had to such data protection principles as may be in force. This includes, in particular, information in the following categories:

- Physical or mental health or medical condition, including dates of absence from work due to illness and the reason for the absence
- Matters relating to pregnancy and maternity leave
- Criminal convictions
- Race and ethnic origin
- Qualifications
- Matters of discipline
- Pensionable pay or contributions
- Age and years of service
- Membership of recognised trade union

I understand that the information may be used for the following purposes:

- Administering sick pay and sick leave schemes
- Managing the absence control policy or capability policy
- Checking suitability and fitness to work at the school
- Administration of pay and payroll functions
- Administering the school and statutory maternity leave and pay schemes
- Managing and maintaining a safe school environment
- Managing duties and obligations under the Disability Discrimination Act
- Training and development purposes
- Management planning
- Negotiations with the trade union or staff representatives
- Redundancy and succession planning
- Curriculum planning and organisation
- Timetable organisation
- Compliance with equality and diversity policies, procedures and legislation

Carrying out checks through DBS (Disclosure and Barring Service; previously 'CRB') or other appropriate mechanisms. I understand that this information will be used only for the purposes set out in the statement above and my consent is conditional upon the School complying with their obligations and duties under the Data Protection Act 1998.

Signed _____ Name _____ (*block capitals)* Date _____

Please return this form when complete to SIMS Office

APPENDIX 2

STAFF GUIDELINES FOR DATA PROTECTION

1. All staff will process data about students on a regular basis, when marking registers, or school work, writing reports or references, or as part of a pastoral or academic supervisory role. The school will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

   - General personal details such as names and address.
   - Details about class attendance, coursework marks and grades and associated comments.
   - Notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views, trade union membership, ethnicity or race is sensitive and can only be collected and processed with the student's consent, e.g. recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

3. All staff have a duty to make sure that they comply with the data protection principles.
   - Accurate.
   - Up-to-date.
   - Fair.
   - Kept and disposed of safely, and in accordance with the School policy.

4. Staff will be responsible for ensuring that all data is kept securely. They are also required, without exception to report breaches to the Data Controller or a member of the SLT.

5. Staff must not disclose personal data to any student (or legally-appointed advocate), unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the School policy.

6. Staff shall not disclose personal data to any other staff member or non-employees except with the authorisation or agreement of the designated data controller, or in line with school policy.

7. Before processing any personal data, all staff should consider the checklist below.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent (or the consent of his/her or appropriate representative/carer)?
- Has the student been told that this type of data will be processed?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Public Facing Operations

Staff involved in "public-facing" operations must ensure that they comply with the Data Protection Act and school Data Protection Policy.

Guidelines for Use of Laptops and Memory Sticks

- Personal data MUST NOT be removed from the premises unless this is essential; if it is essential then any risk should be assessed and sensitive data MUST be encrypted and password protected.
- Laptops and memory sticks which regularly hold sensitive personal data MUST be fully encrypted.
- If only a few files are of sensitive nature it may be feasible to simply encrypt these files rather than the whole disk/stick. This could be done on the laptop or memory stick.

Guidance for Internet/Remote Access of School Data

- Care must be taken when viewing school data via the internet or using remote access, for example, viewing ADDS at home.
- Ensure other people cannot view data which they are not authorised to see. Never save your school password to a home PC or public computer
- Securely end your internet browsing/remote access session.