SkillForce
Heroes in Schools Transforming Lives

DATA PROTECTION POLICY

Document Control
Author: Shaun Pape
Owner: Operations
Version No: 1.1
Issue Date: May 2018
Review Date: May 2019
No. of pages: 28

Contents

General statement of the duties of SkillForce.

The General Data Protection Regulation, (GDPR) 2018 came into force on 25th May 2018. It is concerned with the rights of individuals to gain access to personal information held about them by an organisation or individual within it and the right to challenge the accuracy of data held. The terms of the Regulation relate to data held in any form, including written notes and records, not just to electronic data.

SkillForce acts as the data controller for the data that it collects. SkillForce may also act as a data processor of personal data held by SkillForce, in line with the purposes notified to the Information Commissioner by SkillForce. SkillForce remains the data controller of this data.
This policy applies to personal information held and processed by SkillForce, and sets out its duties under the GDPR 2018, including the duty of its staff, based at Central Services and in schools. It provides guidance on processing, retaining, security and disposal of all personal data held by SkillForce.

SkillForce is required to process personal data regarding staff, consultants, students, their parents and guardians as part of their operation, and shall take all reasonable steps to do so in accordance with this Policy and the principles of the GDPR 2018 ('the GDPR').

SkillForce aims to have transparent systems for holding and processing written personal data. Any reference to personal data in this policy includes reference to sensitive personal data. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

Any individual is entitled to request access to information relating to their personal data held on a relevant filing system by the Charity. A relevant filing system is any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. Personal data can be held in any format (electronic, paper-based, and photographic) from which the individual's data can be readily extracted

In this policy, any reference to students includes current, past or prospective students of our programmes.

The General Data Protection Regulation 2018

SkillForce, has the responsibility to comply with the GDPR. The GDPR applies to information relating to both "personal" and "sensitive personal" data.

Personal Data means data relating to a living individual who can be identified from that data (or from that data and other information in possession of SkillForce). The Charity may process a wide range of personal data of staff, consultants, volunteers and students participating in their programmes as part of their operation. To qualify as personal data, the data must allow you to identify and give information relating to a data subject. Personal data includes facts and any expression of opinion about an individual. Examples of personal data are: names and addresses; email addresses; telephone numbers; medical details; bank details; academic records; disciplinary records; attendance records and references.

Sensitive personal data is defined in the GDPR as information in respect of racial or ethnic origin, political opinions, religious beliefs or "other beliefs of a similar nature", membership of a trade union, physical or mental health, sexual life, criminal convictions and alleged offences. Sensitive personal data can only be processed under strict conditions, including a condition requiring consent of the person concerned to such processing.

In order to comply with the GDPR SkillForce will comply with Article 5 of the GDPR which state that personal data must be:

Principle 1: Personal data will be processed fairly and lawfully.

The collection and disclosure of data is subject to scrutiny and is only 'lawful' if it meets at least one of the following criteria (as specified in Article 5 of the Act):

- With the consent of the data subject; or,
- In performance of a contract (for example to process an application as part of the admissions process); or,
- If there is a legal obligation (for example under prevention of terrorism legislation); or
- For the protection of the vital interests of the individual (for example to prevent injury or other damage to the health of the data subject), or,
- In the legitimate interest of the data controller, unless it is prejudicial to the interests of the individual (for example for the purpose of equal opportunities monitoring).

Personal Data must meet all of the following criteria in order to be processed 'fairly':

- Data will only be collected from persons who have the authority to disclose it. If personal information is collected from a third party, the data subject will be informed of the 'use' of the information.
- Subjects will not be deceived or misled in any matter related to the use of personal data.

In addition to the requirements outlined above, sensitive personal data may only be processed if it also meets at least one of the following criteria (as specified in Article 5 of the Act):

- The data subject has given explicit consent.
- It is necessary to meet requirements of employment law.
- It is necessary to protect the vital interests (i.e. if the situation is a matter of life or death) of the subject or another person.
- The data subject has already manifestly made the information public.
- It is necessary for legal proceedings, obtaining legal advice or defending legal rights.
- It is necessary for the carrying out of official or statutory functions.
- It is necessary for medical purposes.
- It is necessary for equal opportunities.
- It is necessary in order to comply with legislation from any Government organisation.

Principle 2: Personal data will be obtained only for one or more specified and lawful purposes

Data will not be further processed in any manner incompatible with the initial specified purpose or those purposes for which it was obtained. To satisfy the first principle (fair processing) the data subject(s) must not have been misled or deceived as to the reason(s) for processing.

Principle 3: Data must be adequate, relevant and not excessive

Personal information, which is not necessary for the intended processing, must not be acquired, i.e. personal information cannot be collected just because 'it may be useful'.

Principle 4: Data must be accurate and up to date

SkillForce will ensure that there is a system in place to review data for accuracy and to ensure that it is up to date. Procedures are in place to make any amendments requested by a data subject, or a record kept if the amendment is not considered appropriate.

Principle 5: Data must not be kept for longer than required for the purpose

SkillForce will indicate the length of time that data is to be in use and archived for any given purpose. This time period must be seen as justifiable for the particular purpose and in line with any legislation covering the processing.

Information should not be kept any longer than the time period indicated to the data subject. SkillForce will regularly review data held in order to assess whether information is still required. The Act recommends that SkillForce has a retention policy in place to ensure information is retained only for as long as is necessary.

The Data Protection Act recommends that SkillForce has a disposal policy in place to which all staff can refer when they need to dispose of personal information. A disposal record will assist SkillForce in responding to enquiries made under the Data Protection Act.

Before disposing of any data, SkillForce will consider the following key points:

- Any legal requirements (e.g. possible negligence action).
- The length of any appeals procedure relating to the information.
- The number of times in the last two or three years that a particular type of record has been accessed.

Principle 6: Data must be processed in line with individual's rights

This is strongly linked to the first principle of fair and lawful processing. Data subjects have the right to know details of the processing and the right of access to personal information.

A data subject (including a member of staff) has the right to object to data processing relating to them, which is likely to cause damage or distress to that data subject or another person. There are a number of provisos to this right, in particular:

- The damage or distress must result from unwarranted processing, or
- The data subject must not have given consent to the processing, or
- The processing is not necessary for the purposes of fulfilling a contract with the data subject; or for fulfilling a legal obligation of SkillForce, or for protecting the data subject's vital interests.

In addition the Act gives data subjects the right to object to processing used for the purpose of direct marketing and/or wholly automated decision making.

Data subjects have the right to have inaccurate data amended and to block future processing in cases of unlawful/unfair processing. Data Subjects must formally request their rights in writing and their rights are enforceable by the courts.

Principle 7: Data must be processed in a secure manner

SkillForce will guard against unauthorised and unlawful processing, e.g. access, alteration, disclosure or disposal. Appropriate security records must be kept in order to provide an audit trail. Personal information will, so far as possible, be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected; or
- Kept only on disk which itself is kept securely.

When personal data is to be destroyed, paper or microfilm records will be disposed of by shredding or incineration; computer hard disks or floppy disks will be reformatted, over-written or degaussed.

Article 5 (2)

The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Processing personal data

Processing of personal data includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data. Processing also includes transferring data to 3rd parties.

Consent may be required for the processing of personal data unless the processing is necessary for the Charity to undertake their obligations to students and their parents or guardians. Personal data, unless otherwise exempt from restrictions on processing under the GDPR, will only be disclosed to third parties under the terms of this policy or otherwise with the consent of the appropriate individual.

The rights in relation to personal data set out under the GDPR are those of the individual to whom the data relates. The Charity will, in most cases, rely on parental or guardian consent to process data relating to students, and those with 'parental responsibility' are entitled to receive relevant information concerning the student. A student of sufficient maturity and understanding has certain legal rights which the Charity must observe. These include the right to give or withhold consent and certain rights to confidentiality. In exceptional circumstances, if a conflict of interest arises between a parent and a student, the rights of, and duties owed to the student will in most cases take precedence over those of the parent.

Exemptions which allow disclosure of personal data to third parties

There are a number of exemptions in the GDPR which allow disclosure of personal data to third parties, and the processing of personal data by the Charity and its employees, which would otherwise be prohibited under the GDPR. The majority of these exemptions only allow disclosure and processing of personal data where specific conditions are met, namely:

a) the data subjects have given their consent;
b) to safeguard national security;
c) for the prevention or detection of crime;
d) to prevent serious harm to the data subject or a third party;
e) for the assessment of any tax or duty;
f) where it is necessary to exercise a right or obligation conferred or imposed by law upon the Charity (other than an obligation imposed by contract);
g) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

h) for the purpose of obtaining legal advice;

Responsibilities under the GDPR

SkillForce is the data controller under the GDPR.

SkillForce may also act as a data processor of personal data held by SkillForce, in line with the purposes notified to the Information Commissioner by SkillForce. SkillForce remains the data controller of this data.

The Board of Trustees is responsible for the Charity's compliance with the GDPR and ensuring that other SkillForce policies and practices are consistent with this policy. The Executive Board are responsible for ensuring that all staff are aware of their responsibilities under the Act and appropriate training is put in place.

The Executive Team shall nominate a Data Protection Officer with specific duties. (See Appendix A).

Compliance with the GDPR is the responsibility of all members of the Charity and Central Services who process personal information.

Notification

Notification is the responsibility of the Data Protection Officer. Details of the Charity's notification are published on the Information Commissioner's website. Anyone who is, or intends processing data for purposes not included in the Charity's Notification (see below) should seek advice from the Data Protection Officer.

Use of personal data by the Charity

The GDPR requires that the personal data held about students and staff must only be used for specific purposes allowed by law. The Charity holds personal data on its staff and students, including: contact details, assessment results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

The data is used in order to support the delivery of our courses, to monitor and report on progress and to assess how well the Charity as a whole is doing, together with any other uses normally associated with this provision in a Charity environment.

The Charity may make use of limited personal data (such as contact details) relating to students, their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with students.

In particular, SkillForce may:

a) Make use of photographs of students in Charity publications and on the Charity website as set out in the parent consent form.
b) Make personal data, including sensitive personal data, available to staff for planning activities.

Photographs with names identifying students will not be published on the Charity website, etc. without the express permission of the appropriate individual. This permission is gained through the completion and signature of the consent form.

Parents/Carers who do not want their child's photograph or image to appear in any of the Charity's promotional material, or be otherwise published, must also make sure their child knows this.

Students, parents and guardians should be aware that where photographs or other image recordings are taken by family members or friends for personal use, the GDPR will not apply, e.g. where a parent takes a photograph of their child and some friends taking part in the activity.

Disclosure of personal data to third parties

The Charity may receive requests from third parties (i.e. those other than the data subject and employees of the Charity) to disclose personal data it holds about staff or students. This information will not generally be disclosed unless one of the specific exemptions under the GDPR which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Charity.

The following are the most usual reasons that the Charity may have for passing personal data to third parties:

a) to give a confidential reference relating to a member of staff;
b) to publish the results of public examinations or other achievements of students of our courses;
c) to disclose details of a student's medical condition where it is in the student's interests to do so, for example for medical advice, insurance purposes or to organisers of Charity trips;
d) to provide the relevant information to the Government Department e.g. DfES, Ofsted, concerned with national education.

Where the Charity receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure. When members of staff receive enquiries from third parties for personal data, the enquirer should be asked why the information is required. If consent to the disclosure has not been given (and an exception does not apply) then the request should be declined. In normal circumstances information should not be disclosed over the phone to third parties. In most circumstances third parties should be asked to provide documentary evidence to support data requests.

Accuracy of personal data

The Charity will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the Data Protection Officer in writing of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

Rights of access by data subjects to their personal data

Under the GDPR, individuals have a right of access to their personal data held by the Charity. This is known as a "Subject Access Request". A request in writing will be accepted as long as satisfactory identification is given and the information request is clear, not excessive or vexatious.

Requests for access to records (Subject Access Requests)

A Subject Access Request (SAR) must be made in writing. A Personal Data Request Form (Appendix B) must be sent to the applicant within two working days of when the request is received by Central Services.

The Form must be returned to the Data Protection Officer at Central Services. Receipt of the completed request form must be noted on the Central Services SAR log by the DP Officer.

A written response acknowledging the application form must be sent to the applicant within 5 working days of the request.

Responding to requests for access to records

The Data Protection Coordinator will co-ordinate the response to the applicant.

The Charity may also wish to get advice from the Solicitors in relation to a disclosure.

If the applicant's request for access is granted, the GDPR requires such access to be given within one month of the written request being received. This may be extended by a further two months where requests are complex or numerous. If this is the case, we must inform the individual within one month of the receipt of the request and explain why the extension is necessary. The one month period does not begin until:

a) a written application is received by the Data Protection Officer at SkillForce Central Services.
b) SkillForce has received sufficient information to enable it to identify the individual who is seeking access;
c) SkillForce has received sufficient information to enable it to access the information requested.

Where the conditions set out above are fulfilled, in responding to the request, SkillForce must give a description of the personal data that is being processed, the purposes for which the personal data is being processed, and the persons to whom the personal data are or may be disclosed.

SkillForce will also provide, in an intelligible form, a copy of the information held and, where possible, details of the source of the information.

Data subjects are not entitled to information where exemptions to the right of access apply (see below). Moreover, in these circumstances, SkillForce will only give a notification to the data subject that no information has been identified which is required to be supplied under the GDPR.

Note: SkillForce will agree a secure method of releasing the records to the applicant.

Exemptions to access by data subjects

Confidential references given, or to be given by SkillForce, are exempt from access. The Charity will therefore treat as exempt any reference given by them for the purpose of employment, training or financial references.

It should be noted that confidential references received from other parties may also be exempt from disclosure. However, such a reference can be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent, or where disclosure is reasonable in all the circumstances.

An exemption may also be considered in cases where a third party is identified and disclosure may be detrimental to that party.

Collection of data

All forms used by SkillForce to collect personal data about an individual will carry a standard Data Protection notice: as follows:

<I/We consent to SkillForce obtaining, using, holding and disclosing "Personal data" including "sensitive personal data" (such as medical information), for the purposes of safeguarding and promoting the welfare of our child, and where necessary, for the legitimate interests of the Charity and ensuring that all relevant legal obligations of the Charity and ourselves are complied with. I/ We give my/our consent to such processing and disclosure provided that at all times any processing or disclosure of personal data or sensitive personal data is done lawfully and fairly in accordance with the GDPR 2018. >

Retention of data

SkillForce will not keep student and related data for longer than necessary. To this end student records will be securely disposed of 7 years after the student finishes their programme. These details will include Name of student, Date of birth, Address, Telephone number, Email address, Name of parents, Gender of student and Year student joined the programme.

Accident books / logs relating to student accidents should be kept until the child reaches 21 years of age as a claim could be made up to that time.

Staff records will be securely disposed of 7 years after a member of staff leaves SkillForce's employment. Brief details will be retained on all staff indefinitely to satisfy future reference requests. These details will include full name, date of birth, job title, national insurance number and period of employment.

Accident books / logs relating to staff accidents should be kept for 12 years after the member of staff has left the Charity's employment.

Personal details of unsuccessful applicants will be disposed of after 6 months.

Fundraising

Fundraising data will be disposed of after three years of loss of contact.

All data collection will include an opt-in clause allowing the data subject to decide whether to allow direct marketing. This will include newsletters, texts, emails or telephone calling.

All data subjects have the right to contact SkillForce to discontinue any form of direct marketing or request that the data that we hold on them is deleted.

All marketing material that is sent on a legitimate interest basis will have a clear opt out option to prevent further contact with the individual.

Audit

An audit of the Charity's compliance with this policy will be carried out on an annual basis by each Area Manager and other managers at Central Services. This audit will be coordinated by the Data Protection Officer for SkillForce (See Appendix C).

All Area Managers and Central Services Managers must complete the Annual Data Protection Audit Return (Appendix F) and forward this to the Data Protection Officer.

Data Protection Impact Assessment.

A DPIA is a process to systematically analyse the processing and identify and minimise the data protection risks. It must:

describe the processing and your purposes;

- assess necessity and proportionality;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk, but should help to minimise risks and consider whether or not they are justified.

You must do a DPIA for processing that is likely to be high risk.

A DPIA may cover a single processing operation or a group of similar processing operations.

A group of controllers can do a joint DPIA.

The DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material - to individuals or to society at large.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context and purposes of the processing.

Staff Data

The principles of the GDPR described in this policy also apply to staff data held by Area Managers or at Central Services.

Staff are made aware of, and agree to their data being processed by SkillForce by signing their contract of employment.

Sensitive personal data will only be used by SkillForce for legitimate business and management purposes and will not be transferred to third parties without consent.

The Data Protection Officer will address the retention periods in the annual audit. They will also remind appropriate staff of the requirement to dispose of expired data securely.

DBS checks are carried out routinely by SkillForce. Staff Records will only indicate whether a satisfactory or unsatisfactory check has been received. No additional details regarding the DBS check will be held on the staff record.

Appendix A: Roles and Responsibilities

Role of the Data Protection Officer

The role of the Data Protection Officer is to:

- Ensure that the organisation complies with the GDPR 2018, and to ensure that employees are fully informed of their own responsibilities for acting within the law and that the public, including employees, are informed of their rights under the Act.
- Be the nominated officer in the Data Protection register maintained by the Information Commissioner, notify the fact of processing to the Information Commissioner and maintain the accuracy and currency of the organisation's notification
- Co-ordinate GDPR activities (including training).
- Ensure organisational compliance, and conformance with the Data Protection Principles
- Develop, implement and enforce a suitable and relevant Data Protection policy and ensure it is reviewed on an annual basis
- To undertake systematic GDPR compliance audits in accordance with Information Commissioner's audit tool
- Assist with investigations into complaints about breaches of the Act and undertake reporting/remedial action as required. Maintain a log of any incidents and remedial recommendations and actions.
- Maintain a log of and co-ordinate Subject Access Requests.
- Maintain and update own knowledge of developments in Data Protection issues.
- Be a resource for other employees by providing expert advice on the GDPR and related issues.

Appendix B: Personal Data Request Form

SkillForce Personal Data Request Form

Request for information under the GDPR 2018
This form should be completed only if you are requesting personal information relating to yourself or on behalf of a third party.

Please complete in block capitals or type. *(* Required Fields).*

1. Personal details of the person requesting the information.

*	Surname:	
*	Forename:	
*	Address:	
*	Postcode:	
	Telephone number:	
	Email:	

2. Are you the Data Subject *(i.e. the person whose information you are requesting)?*
Please tick the appropriate box.

Yes ☐ *(Please go straight to question 5)*

No ☐

3. Personal details of the Data Subject *(if different from those at section 1).*

*	Surname:	
*	Forename:	
*	Address:	
*	Postcode:	
*	Date of birth:	
	Telephone number:	
	Email:	

4. Please describe your relationship with the Data Subject that leads you to make this request on their behalf.

---

5. Information requested
If you would like to see only specific document(s), please describe these below.

---

6. If you would like a full copy of the personal records held by the Charity, please tick here ☐.

Declaration
I certify that the information given in this application form to the Charity is true. I understand that it will be necessary for SkillForce to confirm my/the Data Subject's identity and it may be necessary to supply more detailed information if required.

Signature: ----------

Print name ----------

Date: ----------

The Data Controller is SkillForce.

The details you provide on this form will only be used in connection with your application for the supply of documents and for statistical purposes.

The completed form should be returned to:

The Data Protection Officer
Edwinstowe House
High Street
Edwinstowe
Nottinghamshire
NG21 9PR

I understand that I will receive acknowledgement of my request within 5 days of receipt. My request will be acted upon within one month in normal circumstances.

Office use only

Received by:	Date:
Forwarded to:	Date:
Date to be completed by:	
Comments:	

Appendix C: Audit Outline

1. Aims of Data Protection Compliance Audits

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis.
- Quality Assurance, ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive.
- Retention, appropriate weeding and deletion of information.
- Documentation on authorised use of systems, e.g. codes of practice, guidelines, etc.
- Compliance with individual's rights, such as subject access.
- To assess the level of compliance with the organisation's own data protection system.
- To identify potential gaps and weaknesses in the data protection system.
- To provide information for data protection system review.

2. Audit Objectives

When carrying out a Data Protection Audit in any area of an organisation the Auditor has three clear objectives:

I. To verify that there is a formal (i.e. documented and up-to-date) data protection system in place in the area.

II. To verify that all the staff in the area involved in data protection:
   a. Are aware of the existence of the data protection system;
   b. Understand the data protection system;
   c. Use the data protection system.

III. To verify that the data protection system in the area actually works and is effective.

3. Areas to be examined include:

- Use of appropriate forms when collecting data.
- Storage of data in accordance with the security policy, e.g. locked cabinets, passwords, etc.
- Data being removed in accordance with policy timescales.
- Subject Access Request process in place.
- Staff training requirements assessed and highlighted.

Appendix D: Glossary of Terms

For the purposes of this Regulation:

1. ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

4. ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

7. ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

8. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. [1]‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. [2]However, public authorities which may receive personal data in the framework

of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

11. 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

13. 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

14. 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

15. 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

16. 'main establishment' means:

    1. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

    2. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

17. 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

18. 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19. ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;

20. ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

21. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

22. ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

    1. the controller or processor is established on the territory of the Member State of that supervisory authority;

    2. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

    3. a complaint has been lodged with that supervisory authority;

23. ‘cross-border processing’ means either:

    1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

    2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

24. ‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

25. ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([1]);

26. ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

APPENDIX E: DATA RETENTION SCHEDULE

1. Child Protection			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
1.1 Child Protection issues.	Education Act 2002, s175, related guidance "Safeguarding Children in Education", -September 2004	D.O.B. +25 years	SECURE DISPOSAL unless legal action is pending
1.2 Allegation of a child protection nature against a member of staff, including where the allegation is unfounded.	Employment Practices Code: Supplementary Guidance 2.13.1. (Records of Disciplinary and Grievance) Education Act 2002 guidance "dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
2.1 Records related to the formulation of HR Policies and an Employee Handbook		Permanent	SECURE DISPOSAL unless legal action is pending
2.2 List of all members of staff and employees and dates of employment		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.3 Employee offer letters, confirmation of employment letters, written particulars of employment , contracts of		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
employment and changes to the terms and conditions			
2.4 Information on benefits per member of staff/employee		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.5 Pension records		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.6 Training records		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.7 Job applications, CVs and interview records	The Information Commissioner's Employment Practices Code, Parts 1.7.5 and 1.7.6	6 months after notifying unsuccessful candidates; 7 years after termination of an employee if the applicant *is* hired	SECURE DISPOSAL unless legal action is pending
2.8 Personnel Files (including all records relating to promotions, demotions, grievance procedures, resignation or termination letters)		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.10 Disciplinary Matters			
2.10.1 Verbal Warning	Employment Relations Act 1998	Records resulting from a verbal warning should be retained on file for 6 months then destroyed.	SECURE DISPOSAL unless legal action is pending
2.10.2 Written Warning	Employment Relations Act 1998	Records resulting from a written warning should be retained on file for 12 months	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
		then destroyed.	
2.10.3 Final Written Warning	Employment Relations Act 1998	Records resulting from a final written warning should be retained on file for 12 months then destroyed.	SECURE DISPOSAL unless legal action is pending
2.11 Job descriptions and performance goals		7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.12 Immigration checks	Immigration, Asylum and Nationality Act 2006	Up to 2 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.13 Records in relation to hours worked and payments made to workers	Section 9, National Minimum Wage Act 1998 Regulation 38, National Minimum Wage Regulations 1999	3 years beginning with the day upon which the pay reference period immediately following that which they relate ends	SECURE DISPOSAL unless legal action is pending
2.14 Records relating to accidents / injury at work.		Date of incident +40 years	SECURE DISPOSAL unless legal action is pending
2.15 Information relating to the member of staff's/employee's exposure to toxic substances (Medical Records to be stored separately in confidential location.)		Permanently	SECURE DISPOSAL unless legal action is pending
2.16 Working time opt-out forms	Regulations 5 and 9, Working Time Regulations 1998	2 years from the date on which they were entered into.	SECURE DISPOSAL unless legal action is pending
2.17 Records to show compliance with the Working Time Regulations 1998	Regulations 5, 7 and 9, Working Time Regulations	2 years after the relevant period.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
	1998		
2.18 Annual leave records		6 years or possibly longer if leave can be carried over from year to year.	SECURE DISPOSAL unless legal action is pending
2.19 Payroll and wage records for companies		6 years from the financial year end in which payments were made.	SECURE DISPOSAL unless legal action is pending
2.20 Maternity records	Regulation 26, Statutory Maternity Pay (General) Regulations 1986	3 years after the end of the tax year in which the maternity pay period ends.	SECURE DISPOSAL unless legal action is pending
2.21 Current bank details		No longer than necessary.	SECURE DISPOSAL unless legal action is pending
2.22 Records of advances for season tickets and loans		While employment continues and up to 6 years after repayment.	SECURE DISPOSAL unless legal action is pending
2.23 Death benefit nomination and revocation forms		While employment continues or up to 6 years after payment of benefit.	SECURE DISPOSAL unless legal action is pending
2.24 Consents for the processing of personal and sensitive data		For as long as the data is being processed and up to 6 years afterwards	SECURE DISPOSAL unless legal action is pending
2.25 Disclosure and Barring Service checks and disclosures of	Rehabilitation of Offenders Act	Should be deleted following	SECURE DISPOSAL unless legal

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes &Actions**
criminal record forms	1974 The Information Commissioner's Employment Practices Code, Parts 1.7.4 and 2.15.3	recruitment process unless assessed as relevant to ongoing employment relationship. The information may include information on any spent conviction permitted under the exceptions order	action is pending
2.26 Emails - SkillForce staff		Mail is retained for 6 months after a member of staff leaves SkillForce	SECURE DISPOSAL unless legal action is pending
2.27 My Documents		My Documents is retained for 6 months after a member of staff leaves SkillForce	SECURE DISPOSAL unless legal action is pending

3. Student records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
3.1 Admission Registers		Date of last entry in the book (or file) +7 years.	SECURE DISPOSAL unless legal action is pending
3.2 Attendance Reports		Date of register + 3 years	SECURE DISPOSAL unless legal action is pending
3.3 Pupil Records			
3.3.1 Primary		All data to be removed 5 years	SECURE DISPOSAL unless legal

3. Student records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
		after pupil has left the Programme.	action is pending
3.3.2 Secondary	Limitation Act 1980	All data except to be removed 5 years after pupil has left the course.	SECURE DISPOSAL unless legal action is pending
3.3.3. Records relating to accidents / injury		Copy given to Charity. Date of incident +40 years.	SECURE DISPOSAL unless legal action is pending
3.4 Assessment Results			
3.4.1 Assessment results		7 years after leaving the Programme	SECURE DISPOSAL unless legal action is pending
3.4.2 Any other records created in the course of contact with pupils		7 years after leaving the Programme	SECURE DISPOSAL unless legal action is pending

4. Complaint Records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
4.1 Any data relating to a complaint, issue or potential complaint or issue relating to: - Any member of staff - any consultant - any act or omission of any member of staff or other employee or any contractor engaged by SkillForce		During the period which the complaint or issue is investigated until final disposition of the matter and thereafter for a period of 7 years	

- anything which happened in or around any premises occupied by the SkillForce			
4.2 Other e-mail any attachments and voice recording (**unless** other provisions of this guide apply requiring longer retention)		For the period of 2 years	Note : Subject to any, longer retention period which may be required under other provisions of this guide

5. Fundraising			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
5.1 Records relating to fundraising including donations from both corporate and individuals will be deleted after three years non contact.	Information Commissioners Office.	Three years following loss of contact.	SECURE DISPOSAL unless legal action is pending

6. Litigation			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
6.1 Records relating to pending, threatened or reasonably anticipated litigation, government investigation, or complaint or other claim		During the period in which the litigation, investigation complaint or claim is contemplated, pending or threatened and until final disposition of the matter and thereafter for a period of 7 years.	SECURE DISPOSAL unless legal action is pending

Appendix F: Data Protection Audit Return

Area : **Year:**

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
1.0	Staff / Student Records					
1.1	Student data is kept in accordance with the data retention policy.					
1.2	Staff data is kept in accordance with the data retention policy.					
1.3	Expired records are disposed of safely and securely by named individuals.					
1.4	All forms used to collect data are identified.					
1.5	All forms used to collect data include the standard SkillForce Data Protection disclaimer.					
1.6	All electronic databases in use, including the users who can access them, are identified.					
1.7	Access to all electronic databases is secured by individual username and password.					
1.8	Passwords protecting access to all electronic databases are changed regularly, e.g. every 90 days.					
1.9	All paper record systems in use, for staff or students, are identified.					
1.10	All paper record systems are secured in accordance with policy guidelines.					
1.11	Staff with access to staff records is documented, controlled and regularly reviewed.					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
1.12	The Accident Book is used for students and records are kept until the child is 21.					
1.13	The Accident Book is used for staff and records are kept for 12 years after member of staff has left.					
1.14	All students, whose parents have opted not to have their photograph used, are clearly identified with the information easily accessible to staff.					
2.0	**Procedures**					
2.1	All third party organisations offering a service on your premises, including the data they collect (if any), are identified.					
2.2	A Subject Access Request (SAR) file is in place to store requests.					
2.3	The SAR process has been tested.					
3.0	**Staff Training**					
3.1	Staff are made aware of SkillForce's Data Protection policy and its implications for them in their work.					
3.2	Staff are made aware of SkillForce's Computer and Electronic Systems policy and its implications for them in their work.					
3.3	Staff are made aware of that they must inform the Charity of any changes to their personal details, e.g. change of address, contact numbers.					

Status Key:

Status	Description
	Policy standard not met.
	Policy standard partially met. Action Plan in place to achieve full compliance.
	Policy standard achieved.

Audit completed by (please print):

Signed:

Position:

Date: