

Policy 02 – GDPR -Data Protection Policy

Revision Number	Page No(s)	Revision Date	Author	Modifications
1.0	All	15/12/15	Steve Henton	First issue of policy
2.0	All	29/03/16	Steve Henton	Entire document reviewed and published.
2.1	All	15/07/16	Sam Taylor	Rebrand onto new template and review.
2.2	All	20/5/17	Mark Urch	Rebranded and name changes, updated inconsistencies
2.3	All	30/06/17	Mark Urch	Updated to reflect the adoption of GDPR.
3	All	15/06/19	Malcolm Caple	Reference to Annex A SOA
4	All	18/06/20	Malcolm Caple	Policy name change & additional wording ref GDPR

Annex A Reference

A.18.1.4 Privacy and protection of personally identifiable information

Smart Apprentices Ltd is committed to a policy of protecting the rights and privacy of individuals, in accordance with the General Data Protection Regulation (GDPR). GDPR contains provisions that the organisation will need to be aware of as data controllers, including provisions intended to enhance the protection of personal data.

GDPR requires that:

Smart Apprentices Ltd needs to process certain information about its staff, customer, suppliers, and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The day to day purchasing and sales of goods
3. The making or receiving of payments as part of day to day trading
4. To contact you about a submission or request for information you have made.
5. In relation to any correspondence we receive from you or any comment or complaint you make about our products or services.
6. Complying with legal obligations and government including local government.



To comply with various legal obligations, including the obligations imposed on it by GDPR Smart Apprentices Ltd must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Responsibility

Responsibilities under GDPR Smart Apprentices Ltd will be the 'data controller' under the terms of the legislation. This means it is ultimately responsible for controlling the use and processing of personal data. The company appoints a Data Protection Officer (DPO) for each site who is available to address any concerns regarding the data held by the company and how it is processed, held, and used.

The Senior Management Team is responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the company.

The Senior Management Team is also responsible for ensuring that the Companies policy is kept up to date. Details of the Smart Apprentices Ltd.'s policy can also be found on their website

Compliance with the legislation is the personal responsibility of all staff at Smart Apprentices Ltd who process personal information.

Individuals who provide personal data to Smart Apprentices Ltd are responsible for ensuring that the information is accurate and up to date.

This policy applies to all staff of Smart Apprentices Ltd and all other computer, network or information users authorised by Smart Apprentices, or any department thereof. It relates to their use of any Smart Apprentices-owned facilities (and those leased by or rented or on loan to Smart Apprentices), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the company network; to all company-owned or licensed data and programs (wherever stored); and to all data and programs provided to Smart Apprentices by sponsors or external agencies (wherever stored).

The policy also relates to paper files and records created for the purposes of Smart Apprentices business. The Data Protection Act 2018 requires every data controller who is processing personal data to notify the Information Commissioner unless they are exempt. Failure to notify is a criminal offence. Smart Apprentices has set up a direct debit to renew our notification each year for the following purposes:

- Staff administration;
- Advertising, marketing and public relations;
- Accounts and records;
- Administration of membership records;
- Advertising, marketing and public relations for others;
- Consultancy and advisory services;
- Education;
- Fundraising;
- Information and databank administration;
- Journalism and media;
- Legal services;
- Processing for not for profit organisations;
- Realising the objectives of a charitable organization or voluntary body;
- Research;
- Trading/sharing in personal information.



Formal record keeping of any changes in the scope of records being kept will be maintained by SA, these records will be made available upon request.

EIGHT DATA PROTECTION PRINCIPLES

Whenever collecting information about people Smart Apprentices agrees to apply the Eight Data Protection Principles:

1 Personal data should be processed fairly and lawfully

Smart Apprentices Ltd will make all reasonable efforts to ensure that individuals who are the focus of personal Identifying information (PII) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

The Company will process the data for the specific and lawful purpose for which it was collected and not further process the data in a manner incompatible with this purpose. The Company will ensure that the reason for which it collected the data originally is the only reason for which it processes that data unless the individual consents to any additional processing before it takes place.

Smart Apprentices Ltd undertakes not to disclose personal data to unauthorised third parties.

Legitimate disclosures may occur in the following instances:

- Where the individual has given their consent to the disclosure.
- The disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual.

CCTV. There are some CCTV systems operating within Smart Apprentices Ltd for the purpose of protecting staff and property. Smart Apprentices Ltd will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

2 Personal data should be obtained only for the purpose specified

The Company will process the data for the specific and lawful purpose for which it was collected and not further process the data in a manner incompatible with this purpose. The Company will ensure that the reason for which it collected the data originally is the only reason for which it processes that data unless the individual consents to any additional processing before it takes place.

3 Data should be adequate, relevant, and not excessive for the purposes required

The Company will ensure that the data is adequate, relevant, and not excessive in relation to the purpose for which it is processed. Smart Apprentices Ltd will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained.



4 Personal data must be accurate and kept up to date

It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and everyone should notify the Company if a change in circumstances mean that the data needs to be updated.

It is the responsibility of the Company to ensure that any notification regarding the change is noted and acted on.

5 Only keep personal data for as long as is necessary (the right to erasure).

Smart Apprentices Ltd undertakes not to retain personal data for longer than is necessary to ensure compliance with GDPR legislation, and other statutory requirements.

This means Smart Apprentices Ltd will undertake a periodic review of the information held and implement a purge process as required.

Smart Apprentices Ltd will dispose of any personal data in a way that protects the rights and privacy of the individual concerned.

6 Data processed in accordance with the rights of data subjects under this act

Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This will be done without delay, and no later than one month.

4. Right to erasure

- We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing



- We will comply with any request to restrict, block, or otherwise suppress the processing of personal data. We will not process this further.

6. Right to data portability

- We will provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We will provide it in a commonly used, machine-readable format.

7. Right to object

- We respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We respect the right of an individual to object to direct marketing, including profiling.
- We respect the right of an individual to object to processing their data for scientific and historical research and statistics.
- Individuals have the right to object to their data being used on grounds relating to their particular situation.

8. Rights in relation to automated decision making and profiling

- We respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

7 Security: appropriate technical and organisational measures should be taken unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data

Data security

We will ensure data is kept secure against loss or misuse. Where other organisations process personal data as a service on our behalf, we will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a [password manager](#) to create and store their passwords.
- Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when they are not being used
- Servers containing personal data will be kept in a secure location, away from general office space
- Data will be regularly backed up in line with the company's backup procedures
- All servers containing sensitive data will be approved and protected by security software
- All possible technical measures will be put in place to keep data secure

8 Personal data shall not be transferred outside the EEA unless that country or territory ensures an adequate level of data protection.

Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) 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. Smart Apprentices Ltd will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so Smart Apprentices Ltd will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If Smart Apprentices Ltd collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Following the changes in EU legislation and the introduction of the GDPR the following principals have also been adopted.

1. Consent
SA will ensure any agreement terms are intelligible and in an easily accessible form, using clear and plain language and ensure it is as easy to withdraw consent as it is to give it
2. Breach Notification
SA will notify any affected party within 72hrs of the identification of a breach and loss of data.
3. Right to Access
All personal data can be made available either through access from colleges/providers or upon request to SA.
4. Right to be Forgotten
 - All data is achieved by the college/providers following this data is excluded from any access or from any processing except to the originating providers.
 - Data will only be kept for a period required to conform with audit requirements
 - As part of the employee leaver process, employees are marked as left and removed from any further processing.
5. Data Portability
SA SLAs provide for control of data transferred from other systems, all data is securely transmitted and stored in accordance with all DP controls.
6. Privacy by Design
SA will ensure privacy by design, ensuring the inclusion of data protection from the onset of the designing of systems



7. Data Protection Officers

SA will ensure a robust process of internal record keeping for all data sets and Andrew Bowley (CTO) is the appointed Data Security Officer

NOTES FOR SMART APPRENTICES

Data Controller (Smart Apprentice's Chief Executive Officer) must provide their identity; inform people what the information is being collected for and any other information necessary. We must get their consent.

We should think in advance about what we wish to do with personal data. I.E.; if we get names and addresses for a specific campaign we should only use that info for that campaign. We should from now on add other purposes to forms. E.g.; I wish to be kept up-to-date with Smart Apprentices activities.

Individuals have a right to see what data is being kept on them, and for what purpose in 40 days. We must be able to provide a meaningful response within that time.

Same principles apply when data is taken out of the office.

If we buy in a mailing list, we cannot use it for any other purpose than the original Data Controller specified. We must check original use before purchasing the list.

WORKING FROM HOME

- Smart Apprentices keeps note of which staff take work home with them.
- If working on something at home and at work, try to keep both sets of information pretty much up to date.
- Home computers should have records removed once project/work records are no longer needed at home.
- Staff agree to keep work taken home secure; to return all work-related material upon the completion /termination of their contract; and the organisations should be informed if information gets into wrong hands.

SPECIAL FUNDING TRACKING REQUIREMENTS AND DATA PROTECTION

- Try not to keep more information than project/tracking requires;
- The more information kept, the more secure it should be;
- If publishing volunteers' details, tell them first;
- Take extra care if records include sensitive data;
- Just keep personal data as long as necessary under funding rules
- Do not keep surplus information.



SECURITY STATEMENT

Smart Apprentices has taken measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage. This includes:

- Adopting an information security policy (please see Smart Apprentice’s Information Security Policy);
- Taking steps to control physical security;
- Putting in place controls on access to information (please see Smart Apprentice’s Password Policy);
- Establishing a business continuity/disaster recovery plan;
- Training all staff on security systems and procedures;
- Detecting and investigating breaches of security should they occur (Please see Incident Reporting Policy);
- Access to data whether current or archived is provided to those individuals who need to use the specified data in performing their responsibilities and functions;
- All data on the network is protected by Avast! anti-virus software that runs on servers and workstations and is updated automatically with on-line downloads from the Avast! Website. This includes alerts whenever a virus is detected;
- Any viral infection that is not immediately dealt with by Avast! is notified to the Chief Technical Officer;
- Any access to Smart Apprentices is protected through our hosting company Azure which has all the latest virus patches etc.
- All user data is backed up automatically on a daily basis by Azure who host the solution for Smart Apprentices, and this can be restored as necessary;
- A full server backup takes place weekly;
- As Azure are a separate company to Smart Apprentices and is 100 miles away from the Smart Apprentices offices, a disaster contingency plan is already in place in case of catastrophic system loss such as fire, flood etc.
- Every page on Smart Apprentices is also SSL certificated for extra protection. Each page contains the prefix https://

Incident Response

GDPR introduces a duty to report certain types of personal data breach to the relevant supervisory authority. Where feasible Smart Apprentices Ltd will do this within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, Smart Apprentices Ltd will also inform those individuals without undue delay.

This policy will be updated to reflect the General Data Protection Regulation (GDPR) May 2018.

Please view the ICO’s website (<https://ico.org.uk>) which provides further details and guidance.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact: Andrew Bowley CTO.

Acknowledgement

I have read and understood the content of this policy.

I am aware of where to find it on the Integrated Management System to ensure I am updated with any amendments to it.

I agree to abide by the content of this policy at all times.

Signature:	Date:
------------	-------



--	--