GDPR Data Protection Policy

Document Number 87

June 2020 V6

SMART AWARDS
Awarding Platform for Smart Qualifications

Beechwood House | Tanners Lane | Berkswell | Coventry | CV7 7DA
T: 02476 421125
E: info@smartawards.co.uk
W: www.smartawards.co.uk

Company Number 9079735 | VAT Number 216 7632 08

SCOPE

1. SMART AWARDS need to collect and use certain types of information about the Individuals or Service Users (known as data subjects) who come into contact with SMART AWARDS in order to carry on our work. We are committed to a policy of protecting the rights and privacy of individuals. This personal information must be collected and dealt with appropriately. Personal data can be held on computers, databases, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, photographs or recorded on other material and there are safeguards to ensure this under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

POLICY STATEMENT

2. The Board of Directors and management of SMART AWARDS, located at Beechwood House, Tanners Lane, Berkswell, Coventry, CV7 7DA are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information SMART AWARDS collects and processes in accordance with the General Data Protection Regulation (GDPR). Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy along with connected processes and procedures.

3. The GDPR and this policy apply to all of SMART AWARDS personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source SMART AWARDS has established objectives for data protection and privacy.

4. The Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to SMART AWARDS activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

5. This policy applies to all Employees/Staff [and interested parties] of SMART AWARDS such as outsourced suppliers. Any breach of the GDPR or this PIMS will be dealt with under SMART AWARDS disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

6. Partners and any third parties working with or for SMART AWARDS, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

7. No third party may access personal data held by SMART AWARDS without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which SMART AWARDS is committed, and which gives SMART AWARDS the right to audit compliance with the agreement.

8. All Employees/Staff of SMART AWARDS [and certain external parties] are expected to comply with this policy. All Employees/Staff, and certain external parties, will receive appropriate training. The consequences of breaching this policy are set out in SMART AWARDS disciplinary policy and in contracts and agreements with third parties.

9. SMART AWARDS consider:
    - any external and internal issues that are relevant to the purpose of SMART AWARDS
    - specific needs and expectations of interested parties
    - organisational objectives and obligations
    - the organisations acceptable level of risk; and
    - any applicable statutory, regulatory or contractual obligations.

Performance management information system (PIMS) Scope Statement

10. SMART AWARDS objectives for compliance with the GDPR and a PIMS:
    - are consistent with this policy
    - are measurable
    - take into account GDPR privacy requirements and the results from risk assessments and risk treatments
    - are monitored
    - are communicated
    - are updated as appropriate

11. In order to achieve these objectives, SMART AWARDS has determined:
    - what will be done
    - what resources will be required
    - who will be responsible
    - when it will be completed
    - how the results will be evaluated

DATA CONTROLLER AND PROCESSOR

12. SMART AWARDS is the Data Controller and Processor under the GDPR, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

13. SMART AWARDS is registered with the Information Commissioner's Office (ICO) to process personal data. As a registered body, SMART AWARDS determine the purposes for which, and the manner in which, personal data is to be processed.

14. SMART AWARDS will conduct a data protection impact assessment (DPIA) for any processing that is likely to pose a high risk to individuals' rights. This will include a description of the planned processing, an analysis of the necessity for it, an assessment of the risks to privacy, and the measures that may be put in place to mitigate the risks to the rights and freedoms of the data subjects.

15. A DPIA must be undertaken whenever there is a change in processes, technology, or new activity within SMART AWARDS. SMART AWARDS will ensure that systems and processes are designed that secure the data, and which ensure that data is managed properly.

DISCLOSURE

16. SMART AWARDS may need to share data with other agencies such as the local authority, funding bodies and other agencies or stakeholders. The data subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows to disclose data (including sensitive data) without the data subject's consent.

17. These are:
    - Carrying out a legal duty
    - The data subject has already made the information public
    - Conducting any legal proceedings, obtaining legal advice or defending any legal rights
    - Monitoring for equal opportunities purposes – i.e. race, disability or religion
    - Providing a confidential service where the data subject's consent cannot be obtained

18. We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. We intend to ensure that personal information is treated lawfully and correctly.

RESPONSIBILITIES

19. SMART AWARDS is the data controller and/or data processor under the GDPR, and is legally responsible for complying with regulations, which means that it determines what purposes personal information held will be used for. This is policy is for product and services offered by Smart Awards. This policy is for all internal and external stakeholders and all those involved with the development, delivery and quality assurance of Smart Awards qualifications. Smart Awards has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it. Smart Awards has the day-to-day responsibility for implementing this policy and for monitoring its use and effectiveness and dealing with any queries on its interpretation.

R	Responsibilities	The person who actually carries out the process or task. The person is responsible for action/implementation. Responsibilities can be shared
A	Accountabilities	The person who is ultimately accountable for the process or task being completed and who has the authority to make decisions, yes or no authority and veto power. Responsible person (s) are accountable to this person. Only one A can be assigned to a task
C	Consulted	The person to be consulted prior to a final decision or action (two-way communication). People who are not directly involved with carrying out the task but are consulted with.
I	Informed	Anyone whose work depends on the process or task and who has to be updated about the progress after a decision or action has been taken (one-way communication).

TASKS	BOARD	CEO	MD	OPS DIRECTOR	QUALITY PORTFOLIO MANAGER	STANDARDS COMPLIANCE OFFICER	QUAL ADMIN OFFICER	IT CONSULT	FINANCE AUDITOR	EQA	NOPS BOARD	CENTRES
Awarding Policies and Process												
GDPR Data Protection	A	R	R	R	R	R	R	R	R	R	R	R
ASSOCIATED TASKS												
Awarding Policies and Process												

GDPR audit	A	R	R	R	R	R	R	I	I	I	I	R
GDPR complaints	A	R	R	R	R	R	R	I	I	I	I	R
GDPR data breach	A	R	R	R	R	R	R	I	I	I	I	R
GDPR portability	A	R	R	R	R	R	R	I	I	I	I	R
GDPR data impact assessment	A	R	R	R	R	R	R	I	I	I	I	R
GDPR data subject consent	A	R	R	R	R	R	R	I	I	I	I	R
GDPR data subject withdrawal	A	R	R	R	R	R	R	I	I	I	I	R
GDPR information security	A	R	R	R	R	R	R	I	I	I	I	R
GDPR manage of third parties	A	R	R	R	R	R	R	I	I	I	I	R
GDPR nonconformity	A	R	R	R	R	R	R	I	I	I	I	R
GDPR privacy statement	A	R	R	R	R	R	R	I	I	I	I	R
GDPR retention of records	A	R	R	R	R	R	R	I	I	I	I	R
GDPR staff training	A	R	R	R	R	R	R	I	I	I	I	R
GDPR subject access request	A	R	R	R	R	R	R	I	I	I	I	R
GDPR data to third countries	A	R	R	R	R	R	R	I	I	I	I	R
GDPR individual user access	A	R	R	R	R	R	R	I	I	I	I	R
Holiday/Sickness Cover												
The MD, CEO and Operations Director cover holiday/sickness and absenteeism for areas where the person is responsible for action/implementation of a task. The MD. CEO and Operations Director hold company wide experience to be able to carry out these tasks and hold no conflicts of interest.												

20. SMART AWARDS will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

21. Fully observe conditions regarding the fair collection and use of information.
    - Meet its legal obligations to specify the purposes for which information is used.
    - Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
    - Ensure the quality of information used.
    - Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR

22. Top Management and all those in managerial or supervisory roles throughout SMART AWARDS are responsible for developing and encouraging good information handling practices within SMART AWARDS.

23. The Data Protection Officer is accountable to the Board of Directors of SMART AWARDS for the management of personal data within SMART AWARDS and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

DATA SUBJECT RIGHTS

- Right to be informed: we shall provide 'fair processing information and publish a privacy note on our website which informs individuals of the data processing credentials.
- Right of access: we will ensure that individuals have the right to see the data we hold on them.
- Right of rectification: If records are inaccurate, a data subject may request to have them changed. Where data is shared with third-parties, we will inform them of any rectifications.
- Right to erasure: Also known as 'the right to be forgotten', data subjects can request deletion of their personal data. Where data is shared with third-parties, we will also inform them of deletion.

24. Right to restrict processing: Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it. We will retain just enough information about the individual to ensure that the restriction is respected in future.

25. Right to data portability: We will allow delegates to securely move, copy or transfer their data. This will be provided, free-of-charge, in a commonly used, machine-readable format.

26. Right to object processing for scientific, historical, or statistical processes: Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

27. Rights in relation to automated decision-making and profiling: Where automated decisions are made without human intervention, data subjects may choose not to be subjected to it and will be offered a human point-of-contact. SMART AWARDS will ensure that every consent is kept and available for inspection.

DATA PROTECTION PRINCIPLES

28. SMART AWARDS will take appropriate technical and organisational security measures to safeguard personal information, ensuring that personal information is not transferred without suitable safeguards. SMART AWARDS will treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information and set out clear procedures for responding to requests for information.

29. SMART AWARDS will adhere to the Principles of General Data Protection regulations (GDPR). We shall deliver information in a way which can be understood by our target audience using appropriate language and branding. We will direct users of our website/products/services to a 'privacy statement' using pop ups, tick-boxes and 'just-in-time' notices or icons in order to highlight transparency, giving the users genuine control and choice, essential to fair processing.

- Lawfulness, fairness and transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.
- Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources. The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.
- Transparently – the GDPR includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

- Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of SMART AWARDS GDPR register of processing
- Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
  The Data Protection Officer is responsible for ensuring that SMART AWARDS do not collect information that is not strictly necessary for the purpose for which it is obtained
  All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer
- The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit/external experts to ensure that collected data continues to be adequate, relevant and not excessive
- Accuracy: Personal data shall be accurate and, where necessary, kept up to date.
  Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

30. The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it. It is also the responsibility of the data subject to ensure that data held by SMART AWARDS is accurate and up to date.

31. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

32. Employees/Staff [/customers/others] should be required to notify SMART AWARDS of any changes in circumstance to enable personal records to be updated accordingly.

33. It is the responsibility of SMART AWARDS to ensure that any notification regarding change of circumstances is recorded and acted upon.

34. The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

35. On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by SMART AWARDS, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.

36. The Data Protection Officer is responsible for responding to requests for rectification from data subjects. The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

37. Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

38. Where personal data is retained beyond the processing date, it will be [minimised/encrypted/pseudonymised] in order to protect the identity of the data subject in the event of a data breach.

39. Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

40. The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

41. Integrity and confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

42. The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of SMART AWARDS controlling or processing operations.

43. In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on SMART AWARDS itself, and any likely reputational damage including the possible loss of customer trust.

44. When assessing appropriate technical measures, the Data Protection Officer will consider the following:
    - Password protection;
    - Automatic locking of idle terminals;
    - Removal of access rights for USB and other memory media;
    - Virus checking software and firewalls;
    - Role-based access rights including those assigned to temporary staff;
    - Encryption of devices that leave the organisations premises such as laptops;
    - Security of local and wide area networks;
    - Privacy enhancing technologies such as pseudonymisation and anonymisation;
    - Identifying appropriate international security standards relevant to SMART AWARDS

45. When assessing appropriate organisational measures, the Data Protection Officer will consider the following:
    - The appropriate training levels throughout SMART AWARDS;
    - Measures that consider the reliability of employees (such as references etc.);
    - The inclusion of data protection in employment contracts;
    - Identification of disciplinary action measures for data breaches;
    - Monitoring of staff for compliance with relevant security standards;
    - Physical access controls to electronic and paper-based records;

- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

46. Accountability: The controller shall be responsible for and be able to demonstrate compliance with the GDPR.

47. The GDPR includes provisions that promote accountability and governance. These complement the GDPRs transparency requirements. The accountability principle requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

48. SMART AWARDS will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

49. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

50. All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

51. Assessment of adequacy by the data controller - In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.
- Exceptions - In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:
- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

52. Data from children (under 16) requires authorisation from a parent or guardian, SMART AWARDS will make all reasonable efforts to obtain this. It is a requirement to notify authorities within 72 hours of any data breach. There'll be a requirement on all organisations to report any personal data breach to the relevant authorities and, in some cases, to the individuals affected by the breach.

GENERAL GUIDELINES

53. SMART AWARDS will, through appropriate management, strict applications of controls ensure:
    - Confidential information is not shared informally
    - Personal data is not disclosed to unauthorised people
    - Collect and process appropriate information, only to the extent that is needed
    - Employees keep all data secure and is only available to those who need it
    - Strong passwords are used and regularly changed
    - Appropriate security measures are in place to safeguard personal data
    - Data is regularly reviewed, updated and archived in line with guidance and schedules
    - When working with personal data, employees ensure screens of their computers are always locked when left unattended
    - Hold good quality of information ensuring accuracy of data
    - ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data
    - Training and assessment materials are kept on secure internal systems that are password protected. Printed assessment materials are locked in secure areas and only available to those intended
    - Data is not transferred outside of the European area without suitable safeguards
    - Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
    - Everyone managing and handling personal information is appropriately trained
    - Everyone managing and handling personal information is appropriately supervised
    - Anybody wanting to make enquiries about personal information knows the process
    - Enquiries are promptly and courteously dealt with
    - Ensure that the rights of people about whom information is held can be fully exercised under the GDPR
    - Methods of handling personal information are clearly described
    - Methods of handling personal information are regularly reviewed, assessed and evaluated
    - Data protection risks are monitored through SMART AWARDS risk register
    - Any breach of the rules and procedures identified in this policy is a potential breach of the Code of Conduct and may lead to disciplinary action.

DATA PROTECTION OFFICER

54. The Data Protection Officer (CEO) will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- Dealing promptly and courteously with any enquiries about handling personal information
- Describe clearly how we handles personal information
- Will regularly review and audit the ways it holds, manages and uses personal information
- Awareness of data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies, in line with schedule
- Handling data protection questions and dealing with customer requests
- Checking for sensitive data in any contracts or agreements with third parties
- Ensuring all systems, services and equipment meet acceptable security standards
- Preform regular hardware and software checks and scans
- Evaluating any third-party services for the purpose of storing or processing data
- Approve any data protection statements attached to e-mails, letters, communication
- Ensure marketing initiatives comply with the data protection principles
- Will regularly assess and evaluate its methods and performance in relation to handling personal information
- Ensures measures are in place that consider the reliability of employees (such as references etc.)
- Ensures the inclusion of data protection in employment contracts
- Monitoring of staff for compliance with relevant security standards
- Adoption of a clear desk policy
- Ensures the storing of paper-based data in lockable fire-proof cabinets
- Restricting the use of portable electronic devices outside of the workplace
- Restricting the use of employee's own personal devices being used in the workplace
- Adopting clear rules about passwords
- Making regular backups of personal data and storing the media off-site
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

DATA COLLECTION: INFORMED CONSENT

55. Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent. We will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

56. When collecting data, SMART AWARDS will ensure that the Individual/Service User:

- Clearly understands why the information is needed

- Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

57. Where SMART AWARDS provide online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

DATA SHARING

58. All documents created by SMART AWARDS are checked for accessibility and compatibility prior to pubic sharing; documents are also inspected for sensitive and personal data within:
    - Comments, revisions, version, annotations
    - Document properties and personal information
    - Customised ML data
    - Invisible content
    - Hidden text.

HANDLING DATA AND DATA SECURITY

59. All Employees/Staff are responsible for ensuring that any personal data that SMART AWARDS holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by SMART AWARDS to receive that information and has entered into a confidentiality agreement.

60. All staff must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper or in a computer or recorded by some other means.

61. Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the GDPR.

62. It is therefore important the all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data.

63. Email: All staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or, printed and stored securely. The original email should then be deleted from the personal mailbox and any "deleted items" box, either immediately or when it has ceased to be of use. Emails that contain

personal information which is no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

64. Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:
    - If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject or impersonating someone with a right of access.
    - Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.

65. Laptops and Portable Devices:
    - All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program.
    - Ensure your laptop is locked (password protect) when left unattended, even for short periods of time.
    - When travelling in a car, make sure the laptop is out of site, preferably in the boot.
    - If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.
    - Never leave laptops or portable devices in your vehicle overnight.
    - Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.
    - Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of SMART AWARDS.
    - All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.
    - When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

66. All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security and must be kept:
    - in a lockable room with controlled access; and/or
    - in a locked drawer or filing cabinet; and/or
    - if computerised, password protected
    - stored on (removable) computer media which are encrypted

67. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with [procedure reference.

68. Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

69. Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

DATA SECURITY STORAGE

70. Information and records relating to service users will be stored securely and will only be accessible to authorised staff. Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately. It is SMART AWARDS responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

71. Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable) or processed for safe storage or disposal. Always lock (password protect) your computer or laptop when left unattended; this is especially important when using your laptop away from the office.

72. Passwords: Do not use passwords that are easy to guess. Make sure all of your passwords contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length. Protect Your Password: Common sense rules for passwords are; do not give out your password; do not write your password somewhere on your laptop; do not keep it written on something stored in the laptop case.

73. SMART AWARDS will ensure:
    - Paper, CD, DVD files are kept in a locked drawer, when not required
    - Printouts are not left where unauthorised people could see them
    - Data printouts are shredded and disposed of securely when no longer required
    - Electronic data is protected from unauthorised access and accidental deletion
    - Passwords are changed regularly
    - Data is backed up regularly
    - Servers and computers are protected by approved security software
    - Data is held in as few places as necessary
    - Makes every effort to ensure that data held is accurate and kept up-to-date
    - Regularly review data that is collected and cleansing of databases
    - Regular archiving of data.

DATA ACCESS AND ACCURACY

74. All Individuals/Service Users have the right to access the information SMART AWARDS holds about them. SMART AWARDS will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes. In addition, SMART AWARDS will ensure that:
    - It has a Data Protection Officer for ensuring compliance with Data Protection
    - Everyone processing personal information understands that they are contractually responsible for following good data protection practice
    - Everyone processing personal information is appropriately trained to do so

- Everyone processing personal information is appropriately supervised
- Anybody handling personal information knows what to do in the event of an enquiry
- It deals promptly and courteously with any enquiries about personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it holds, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information

SUBJECT ACCESS REQUEST (SAR)

75. An individual is entitled to be given a description of the data being processed or held about them and to be provided with the information constituting personal data and the source.

76. SMART AWARDS will supply information where:
    - A request in writing has been made
    - We are satisfied as to the identity of the applicant
    - We are able to locate the requisite data.

77. A subject access request (SAR) is a request for personal information that SMART AWARDS may hold about a data subject i.e. an individual. If an individual wish to exercise their subject access right, the request must be made in writing. The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of processing of their personal data. Under the GDPR individuals have the right to obtain confirmation as to whether personal data about them is being processed.

78. If personal information is being processed, they are entitled to access:
    - The reasons why their data is being processed
    - The description of the personal data concerning them
    - A copy of all records including e-mails where they are mentioned
    - Information about anyone who has received or will receive their personal data
    - Details of the origin of their data if it was not collected from them.

79. Under the GDPR, a request for personal information is free unless the request is 'manifestly unfounded or excessive.

80. Response time: SMART AWARDS will respond to SAR requests within 40 days of receipt of the written request. Under the GDPR, SMART AWARDS must respond to SARs within one month of receipt. This deadline can be extended by a further two months where there are a number of requests or the request is complex, but you must contact the individual within a month of receipt, explaining why the extension is necessary.

81. Provision of Information: Individuals can make a SAR electronically. If they do so, the information provided should be in a commonly-used electronic format, unless otherwise requested. SMART AWARDS will verify the individual's identity prior to granting access to information. In responding to a subject access request, SMART AWARDS will advise the data subject of:
    - The purposes of the processing
    - The categories of personal data concerned

- Who are the recipients to whom SMART AWARDS discloses the information
- Where possible, how long you will hold onto the information or what categories SMART AWARDS uses to decide how long the personal information will be held for
- The right to request rectification, erasure or restriction of the processing
- The right to lodge a complaint to the ICO
- Where the personal data are not collected from the data subject, the source from where SMART AWARDS obtained the data
- The existence of any automated decision-making.

82. Process: In handling a subject access request, the basic process is:
    - Consider the scope of the request to determine exactly what information is being requested
    - Undertake a thorough search for all personal data within the scope of the request and collate all information that may potentially have to be disclosed
    - Consider whether any exemptions to disclosure apply
    - Once the information that will be disclosed has been identified, consider the appropriate form of disclosure
    - Disclose the information to the applicant or the applicant's nominated representative

83. Exemptions: There are exemptions which mean that personal data within the scope of a subject access request can legitimately be withheld. The main exemptions which may need to be considered are:

84. Information containing personal data about a third party: Management information (personal data that is processed for management forecasting or management planning). Negotiations with the applicant (a record of intentions in negotiations with the applicant).

85. A person making a subject access request only has the right to see their own personal data, rather than a right to see copies of the documents that contain their personal data. Where complying with the request would lead to disclosing data about another identifiable person we are not able to comply unless the other individual has consented, or it is reasonable to comply without consent.

86. Transparency: GDPR focuses on the importance of transparency. Consent must be based on a written explanation couched in clear and plain language in an accessible form. This is a list of information to be included:
    - The controller's identity and contact information;
    - The Data Protection Officer's (DPO) contact information;
    - The purposes and legal basis of the processing;
    - Details of the legitimate interests (if relied upon);
    - Recipients of the personal data;
    - Any intended transfer to a non-EU country and why;
    - How long the data will be stored;
    - Data subject rights;
    - Ability to withdraw consent;
    - Right to lodge a complaint and who to go to;
    - Whether provision of data is required and consequences for failure;
    - Whether automated decision-making is involved and the consequences to the data subject.

DESTROYING PERSONAL DATA

87. Personal data should only be kept for as long as it is needed i.e. only keep that data for the duration required and securely dispose of once the period is complete.

RISKS

88. The GDPR requires the controller and the processor to manage personally identifiable information security and to identify risks appropriate to the severity. This includes risks to individuals: the potential for damage or distress and risks to SMART AWARDS: financial and/or reputational impact of a data breach.

89. Risks can be:
    - Inaccurate, insufficient or out-of-date personally identifiable information
    - Personally identifiable information Kept for too long
    - Excessive or irrelevant personally identifiable information
    - Personally identifiable information disclosed to the wrong people
    - Insecurely transmitted/stored personally identifiable information
    - Personally identifiable information used in ways that are unacceptable or unexpected

90. Risk Level 1: Low risk of tangible or intangible harm if compromised – E.g., middle name, postal code. A very limited number of individuals' PII may be exposed, and/or PII is of limited sensitivity such that the exposure would cause minimal distress or inconvenience, requiring few or no corrective actions on the part of the individual and/or the program. The perception that privacy is being intruded upon is limited, and/or mitigation factors in place make the likelihood of exposure minimal.

91. Risk Level 2: Moderate risk of tangible or intangible harm if compromised – E.g., driver's license number. Numerous individuals' PII may be exposed; and/or PII is of sensitivity such that exposure would cause significant distress or inconvenience requiring some corrective actions on the part of the individual and/or the program. The perception that privacy is being intruded upon is likely, and/or there is a strong possibility that adverse events will occur if no additional corrective measures are taken.

92. Risk Level 3: High risk of tangible harm if compromised – E.g., National Insurance Number. A very large number of individuals' PII may be exposed, and/or the nature of the PII is of high sensitivity such that exposure would cause extreme distress (e.g., vulnerability to blackmail) or inconvenience (e.g., identity theft) requiring extensive corrective actions on the part of the individual and/or the program. The perception that privacy is being intruded upon is extremely likely, and/or it is nearly certain that adverse events will occur if no additional corrective measures are taken.

DATA PROTECTION AND THE LAW

93. The Data Protection Act 2018. This will be superseded by General Data Protection Regulation which comes into force on May 25th, 2018.

94. The GDPR is applied to organisations that are either controllers of the data or those processing the data. As in the GDPR if you are a controller you are responsible for how and why personal data is processed and as a processor you are responsible to act on the controller's behalf. However, in the

GDPR the processor now has a specific legal obligation to maintain records on what personal data they are processing and the processing activities. Therefore, under GDPR both the controller and processor now have defined legal responsibilities.

95. In the GDPR, personal data has been redefined and is now covers a much wider scope, including new areas such as IP addresses, CCTV, biometrics. The GDPR also covers a 'special category of personal data, referred to as sensitive data and may only be processed only within a limited number of circumstances.

96. GDPR Implementation Steps: SMART AWARDS will ensure
    - Awareness - All staff are aware and trained of the impact of the new GDPR regulations
    - Data Protection Officer – A designated person will take responsibility for compliance. This person will be sufficiently competent and have sufficient independence to be able to be effective in the role of the Data Protection Officer.
    - Information We Hold – A mapping of personal data held and why we hold it, where it came from and who we might share it with, how it is held, and how secure it is. An audit of storage and security, including passwords, shared uses, firewalls etc, laptops, smartphones, iPads, memory sticks and personal equipment used away from the office and in homes will be included.
    - Communicating Privacy Information –Our privacy notices to be reviewed and plans made to make any changes needed.
    - Individual's Rights - Procedures to be checked to ensure that individuals' right are covered, including how we delete individual's data, and how we provide them with data electronically.
    - Subject Access Requests (SAR) - Design and implement a SAR template so that you can ensure that all requirements of a response to a SAR are compliant under the GDPR.
    - Lawful Basis for Processing Personal Data - Identify, document and update privacy notice to explain
    - Consent - Review how we seek, record and manage consent, and make any changes needed. Refresh existing consents where necessary. All consents must be kept and accessible.
    - Children - Put systems in place to verify ages and obtain parental/ guardian consent where necessary
    - Data Breaches Put systems in place to detect and report and investigate any breaches
    - Data Protection Impact Assessments – undertake an impact assessment
    - Six lawful grounds for data processing
    - Consent of the data subject
    - Processing is necessary for the performance of a contract with the data subject, or to take steps to enter into a contract
    - Processing is necessary for compliance with a legal obligation
    - Processing is necessary to protect the vital interests of a data subject, or another person
    - Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
    - Necessary for the purposes of legitimate interests pursued by the controller, or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

97. Direct marketing: The GDPR states, 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.' This may be where consent is not viable or not preferred, though organisations will still need to show that there is a balance of interests – their own and those of the person receiving the marketing. Any individual can object to direct marketing.

98. Web analytics: For example, a social media platform using diagnostic analytics to assess the number of visitors, posts, page views, reviews and followers in order to optimise future marketing campaigns.

99. Websites and apps using third-party analytics platforms like Google Analytics etc. will still need consent (even if, for the techies amongst you, the cookie is technically served from a first-party domain – third party here refers to the provider of the analytics service, not the domain from which the cookie is served).

100. Definitions used by the organisation (drawn from the GDPR)

The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

101. The GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

102. Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

103. Personal data – 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.

104. Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

105. Data controller – 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.

106. Data subject – any living individual who is the subject of personal data held by an organisation.

107. Processing – 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.

108. Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

109. Personal data breach – 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

110. Data subject consent - 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.

111. Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

112. Third party – 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.

113. Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

ARCHIVING AND RETENTION

114. SMART AWARDS have an obligation, in line with the data protection policy, to implement and preserve good archiving procedures and processes. Archival records can be in any format; they can exist electronically or paper versions.

115. Files are summarised as:

- Operational files - that are in use daily
- Reference files - that are not in use daily, but are used for reference
- Inactive files - that are no longer active
- Remove files - that are removed after a period of inactiveness
- Preserved files – that are preserved permanently or for a specified length of time.

116. SMART AWARDS aim to ensure:

- All records that are kept as archives will be included in a records retention log

- All records that are kept as archives will have a review date
- The length of their retention will be appropriate to the record – normally 7 years
- Adhere as far as possible to BSI recommendations for the keeping of its archival records
- Individual staff members are responsible for the management of archival records in their areas of work.

117. Email archive and retention
- Messages will move to the online archive 18 months from the original send/receive date
- Messages will be deleted from the online archive 5 years from the original send/receive date
- Exceptions: Items in 'Deleted Items', 'RSS Feeds', and 'Sync Issues' folders will be deleted after 90 days.
- Electronic archive folders will be backed up regularly to ensure that they do not get lost.

INFORMATION ASSET REGISTER/DATA INVENTORY

118. SMART AWARDS has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project.

119. SMART AWARDS data inventory and data flow determine:
- business processes that use personal data
- source of personal data
- volume of data subjects
- description of each item of personal data
- processing activity
- maintains the inventory of data categories of personal data processed
- documents the purpose(s) for which each category of personal data is used
- recipients, and potential recipients, of the personal data
- the role of the SMART AWARDS throughout the data flow
- key systems and repositories
- any data transfers; and
- all retention and disposal requirements.

REVIEW OF THIS POLICY

This policy is reviewed and revised annually in response to feedback, changes in legislation and guidance from the regulators to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).