GSS – General Data Protection Policy

GSS is committed to high standards of information security, privacy and transparency. We place a high priority on protecting and managing data in accordance with current Data protection standards and new EU General Data protection laws which come into force on 25th May 2018. GSS will comply with all applicable GDPR regulations when they take effect including as a data processor, while also working closely with our customers and partners (Data subjects) to meet contractual obligations for our procedures and services. Our team of experienced consultants, Management and support staff will work to ensure we process all data in accordance with GDPR procedures and are committed to ensure compliance at all times.

GSS acknowledge and agree that any personal data that we handle will be processed in accordance with all applicable data protection laws in force at the time.

Overall

The overarching principle of this policy is that;

- All data collected and/or stored by GSS is done so for the sole purposes of GSS's business and an individual's relationship with GSS and or its partner organisations. This will include, but is not limited to, internal marketing of events, notification of relevant information, educational/training, employability, quality standards, CPD and contractual compliance. Individual's personal data will not be shared with any third party without prior written consent (unless where contracted to do so and with the knowledge of the individuals concerned).
- No member of staff will share any personal data with a third party without the prior consent of the individual. This includes, but is not limited to Name, address, email address and phone details.
- All GSS Staff will sign and attend training in relation to understanding the governing principles of GDPR and this will form part of all staff induction and training, current and future whether permanent, temporary or contract.

Data Protection Controller

GSS has appointed a Data controller in Richard Wood, Director who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the Data Protection Act 1998, the Freedom of Information Act 2000 and the protections of Freedoms Act 2002 which are also relevant to this policy.

General Principles

GSS shall so far as is reasonably practical comply with the Data protection principles contained in the Data Protection act to ensure all data is

- Fairly and lawfully processed
- Adequate, relevant and not excessive

- Accurate and up to date
- Must not be kept for longer than necessary
- Processed in accordance with the data subjects rights
- Secure
- Not transferred to other countries without adequate protection

The General Data Protection Policy is structured in accordance with the recommendations based on the control guidelines set out in the industry standard ISO 27001.

This overall document also has a set of other sub-policy documents which together constitute the Information Security Policy of GSS UK Ltd. All of these documents are of equal standing and can be taken in conjunction with or alongside this policy.

Information Security Principles

For the avoidance of doubt GSS adopts the following which continue to underpin this policy:

1. Information will be protected in line with all relevant GSS's policies and legislation, notably those relating to data protection, human rights and freedom of information.

2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset

3. Information will be made available solely to those who have a legitimate need for access.

4. All information will be classified according to an appropriate level of security.

5. The integrity of information will be maintained at all times.

6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.

7. Information will be protected against unauthorised access and only individuals who have been appropriately assessed, vetted and security checked will have access to sensitive data
8. We must always ensure that paper records are kept securely and managed effectively and are kept in a secure place with lockable cabinets, cupboards etc and accessed by those with authority only.
9. Information pertaining to GSS's business including customer data, databases, emails and confidential information will NOT be stored on any external personal devices at any time under any circumstances
10. Compliance with the Information Security policy will be enforced.

11. Before any new systems are introduced, a risk assessment process will be carried out which will include an assessment of the legal obligations that may arise from the use of the system. These legal obligations will be documented and a named system controller, with responsibility for updating that information, will be identified.

1. Third Party Access

All third parties who are given access to the organisation's information systems, whether suppliers, customers, contractors or otherwise, must agree to follow the organisation's information handling, retention and security policies. A copy of the confidential and privacy policy and the third party's role in ensuring compliance will be provided to any such third party, prior to their being granted access.

The organisation will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, GSS may require external suppliers of services to sign a confidentiality agreement to protect its information assets which may form party of any contractual agreements between GSS and the third party

Persons responsible for agreeing maintenance and supporting contracts will ensure that the contracts being signed are in accord with the content and spirit of GSS's security policies.

All contracts with external suppliers for the supply of services to GSS must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier/organisation or individual.

2. Backup and system

GSS will ensure that appropriate backup and system recovery procedures are in place. Backup of GSS's data and the ability to recover this is an important priority. GSS's Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business and is conducted diligently to ensure compliance with our internal and external Contracts.

3. Physical Access to information

Areas and offices where Confidential or Restricted information is processed shall be given an appropriate level of physical security and access control. GSS's Head office is located within a secure building with key fob entry to all areas. Staffs with authorisation to enter such areas are provided with information on the potential security risks in the area and the measures used to control them.

All GSS's staff who have access to data must have signed and agree to the protection of that data and understand and abide by the codes of conduct in the sub documents supplied.

Data used for the purpose of delivering GSS's business must be accessed from GSS supplied or any other device authorised in writing by Richard Wood.

When sending out information on behalf of GSS or it partner organisations to customers whether in a single email or multiple adherence to GSS Confidentiality policy must be adhered to.

Under no circumstances will information pertaining to GSS, customers, clients, or business information be stored on any devices other than those supplied by GSS.

Information pertaining to GSS's business must not be downloaded, stored or saved on any personal device at any time and for any purpose.

Where sensitive or protected data is accessed from any non GSS supplied device any such device is subject to the same security procedures as GSS supplied devices. Written authorisation must be obtained from Richard Wood to access any data held on private networks, cloud based storage, cloud based databases, remote email access or any other similar electronic data repository.

How we use information

GSS will collate information from customers (Data subjects) for the purpose of providing services to them usually within employability or training capacity. The information will have been provided by the customer them self or our partner organisations such as Central and local government agencies . The information is used to establish customer eligibility for our services, right to receive services under government funded programmes, authenticity and for GSS to comply with contractual and legal obligations.

GSS also keep information from prospective applications and staff details which all fall under the general principles of data protection as detailed above.

How we store information

All personal data is stored appropriately and all members of staff are responsible for ensuring that any personal data which we hold is kept securely and not disclosed to any unauthorised third parties.

GSS will ensure that all personal data is accessible only to those who have a valid reason for using it. GSS will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely with controlled access):

- Password protecting personal data held electronically.
- Archiving personal data which are then kept securely (lockable cabinet).
- Placing any PCs or terminals that show personal data so that they are not visible except to authorised staff.
- Ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, GSS will put in place appropriate measures for the deletion of personal data, manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible destroyed physically. GSS use a secure waste management organisation and keep records of this.

This policy also applies to GSS staff who process personal data 'off-site', e.g. when working from home or alternate premises ie, DWP premises, and in these circumstances additional care must be taken regarding the security of the data.

Your Rights

Data subjects have the right at any time to ask for a copy of the information that we hold about them. Individuals wishing to exercise this right should apply in writing to GSS's Management and any such requests will be complied with within 28 working days within the guidelines of disclosure and subject to verification of individual request.

In addition to the right of access to your information data subjects will also have the following rights

- Right to Erasure
- Right to Restriction of processing
- Right to rectification
- Right to restrict processing
- Right to data portability
- Right to withdraw consent

If there are any concerns about the way GSS are collating and using personal data concerns can be raised at any time in the first instance to GSS's Management team or Directors

- Sonia Benjamin
- Richard Wood

Or directly to Information Commissioners Office at https://ico.org.uk/concerns

1. Governance

Responsibility for the production, maintenance and communication of this policy document and all sub-policy documents will be the responsibility of the IT Security Manager alongside GSS Directors.

All documents constituting to and or related to the Information Security Policy will be reviewed annually. It is the responsibility of the IT Security Manager and GSS Directors to ensure that these reviews take place. It is also the responsibility of GSS's Directors to ensure that the policy set is and remains internally consistent.

I …….. commit to abide by this policy and ensure that any breaches or potential breaches to this could result in Disciplinary procedures or breach of contract for services action against me. I understand my obligations to ensure that Information and Data is protected, secure and in line with the information contained within.

Signed:…… Date……

Review

This policy will be reviewed and updated as necessary to reflect best practice, future amendments to the General Data protection Regulations (GDPR) May 2018 and the Data protection act.

Any breaches to the above could constitute gross misconduct and where found, individuals could be subject to disciplinary procedures accordingly.

This policy is not exhaustive and is in conjunction with GSS Information and Data Security policy, GSS confidentiality policy and GSS Diversity.

Signed by Sonia Benjamin
Director
17.07. 2018
Updated v2