E-Safety Policy

This policy, procedure and guidelines have been produced as part of a framework for the protection of all in relation to e-safety. GSS (UK) Ltd are committed to ensuring the appropriate Safety of its staff customers, partners and others who may use technology within the realms of work or training through GSS E-portals or when working with or on behalf of GSS.

The internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication and resources helps GSS employess and learners learn from each other and from a wide range of diverse sources. This can stimulate discussion, create discussion and promote creativity and increase awareness to promote effective, diverse, and up-to-date learning. At all times learners, staff and all those involved in work with GSS should have an entitlement to safe internet access at all times. The requirement to ensure that all people are able to use the ineternet and related communication technologies approproiately and safely is addressed as a wider duty of care to which all work underaken from GSS is bound.

DEFINITIONS

E-Safety is defined as awareness, practice and training of individuals together with IT infrastructure security and infrastucture security and integrity to ensure the safe use of on-line technologies thus maintaining both an individual physical and psychological welbeing and safety as well as GSS organisational reputation.

TECHNOLOGIES

ICT/IT in the 21st Century has an all-encompassing role. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in work places, learning institutes and centres where GSS may conduct business include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

RESPONSIBILITIES

- All staff (including Associates, agency staff, temporary and contract) and Management working on behalf of the organisation have a duty to promote E-safety at all times.

- Staff and management may receive information of breaches to our e-safety policy and those who may be at risk with regards to it. This policy will enable staff to make informed and confident responses to specific issues if they arise.

IMPLEMENTATION ARRANGEMENTS

The roles and responsibilities of staff in implementation of this policy and procedures are set out clearly in the procedure. All new members of staff are made aware of the policy and procedures during formal staff induction process. Updated and amended procedures will be disseminated and reinforced in training sessions, team meetings and via email communications. Staff and learners have access to this policy at Induction, and is available on GSS website and through the intranet.

MONITORING AND REVIEW

GSS Directors alongside GSS's IT Consultant will be responsible for monitoring the effectiveness of the policy. Any serious weakness will be reported to Sonia Benjamin-Leach,Safeguarding Manager, who has the responsibility of ensuring the overall effectiveness of the policy.

Due to the ever changing nature of Information and Communication Technologies, the e-Safety Policy will be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-Safety, organisational or management changes or incidents that have taken place.

SUPPORTING AND RELATED DOCUMENTS

- GSS Safeguarding Policy
- GSS IT and Data Security Policy
- GSS Internet Usage Policy
- GSS Confidentiality Policy
- GSS GDPR policy

PROCEDURE

The following lays out the roles and procedures for e-safety of individuals and groups within GSS:

GSS Directors

GSS Directors has overall responsibility for all matters relating to safety, including e-Safety. This responsibility includes ensuring that management is addressed through comprehensive policies and procedures that are effectively implemented and appropriately resourced within the overall financial position of the organisation

GSS Management

GSS Managers in conjunction with GSS Directors are also responsible for ensuring that this policy is understood by all employees and fully implemented within their area(s) of responsibility. They are responsible for ensuring that within their areas there are effective arrangements in place for the prompt reporting and management of any adverse incidents.

IT Consultant

GSS IT Consultant is responsible for ensuring:

- That the IT infrastructure is secure and is not open to misuse or malicious attack.
- That GSS media systems meets the e-Safety technical requirements outlined in the Internet Usage Policy and any GSS networks through a properly enforced password protection policy, in which passwords are regularly changed.
- GSS's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- GSS keeps up-to-date with e-Safety technical information in order to effectively carry out its e-Safety role and to inform and update others as relevant.
- That any concerns raised over the use of the network/remote access/email will be investigated in accordance with this policy.
- That monitoring software/systems are implemented and updated as agreed, in line with other GSS policies as detailed previously.
- That all systems meet with Cyber essentials plus guidelines and adhere to strict regulations in terms of security.

Employees

Employees are responsible for ensuring that:

- They have an up to date awareness of e-Safety matters and of the current e-Safety Policy and supporting documents.
- They have read, understood and signed the Induction statement and or Policy updates that outlines the agreement to this policy and all others related to it
- They report any suspected misuse or problem to the appropriate person, in line with the Policy.
- Digital communications whether internal or external via email should be on a professional level and only carried out using official GSS systems.
- E-Safety issues are embedded in all aspects of our work for staff, learners, applicants customers and indeed all end users as well as other GSS activities.
- They monitor IT activities in provisions, sessions, lessons and any extended GSS activities.
- They are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement GSS policies with regard to these devices.
- In lessons/provisions where internet use is pre-planned learner/customers are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. (please also see Internet Usage Policy)

Designated Safeguarding Person

- The Designated Safeguarding Person Sonia Benjamin-Leach has day-to-day responsibility for e-Safety, and is aware of the potential for serious safeguarding issues arising from:
    - Sharing of personal data
    - Access to illegal / inappropriate materials
    - Inappropriate on-line contact with adults / strangers

- Potential or actual incidents of grooming
- Cyber-bullying

Learners /Customers

- Are responsible for using IT systems in accordance with their Learner agreements, which they will be expected to sign before being given access to GSS systems
- Have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (please see GSS Plagiarism Policy)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-Safety practice when using digital technologies and realise that GSS's e-Safety Agreement covers their actions outside of GSS's locations whilst working under the direction of GSS.

MANAGING SYSTEMS

Information system security

- The security of GSS's IT systems will be reviewed regularly in line with GDPR and Cyber Essentials
- Virus protection will be installed and updated regularly.
- GSS and working partner organisation uses broadband with its firewall and filters.
- Unknown or non-authroised hardware must not be utulised for GSS's business actitivites unlss pre-arranged and authorised by GSS Directors. This use of unknown/unauthorised disks, USB sticks or other external devices in GSS hardware is strictly forbidden
- Using unauthorised external devices to save customer information or GSS sensitive information is also strictly forbidden

E-mail

- GSS staff may only use approved e-mail accounts on the GSS system. Staff, Consultant or those working on behalf of GSS are not allowed access to personal e-mail accounts or chat rooms whilst working on GSS business.
- All staff must immediately tell GSS Directors if they receive offensive e-mail.
- All Staff, Consultants, Learners and Customers must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on GSS's headed paper.
- The forwarding of chain letters/emails/correspondence is not permitted.
- The contact details on the Web site should be the GSS, e-mail and telephone number. Staff, Consultants, customers and learners personal information will never be published.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Staff, Consultant, learners and customers are advised never to give out personal details of any kind which may identify them or their location. Examples would include last name, address, mobile or landline phone numbers, GSS IM address, personal e-mail address, names of friends, specific interests and clubs etc.

Managing filtering

- GSS will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If anyone discovers unsuitable sites, the URL, time and date must be reported to the E-Safety officer to be blocked
- GSS Directors will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video-conferencing

- IP video-conferencing should use the GSS broadband network to ensure quality of service and security rather than the Internet.
- External IP addresses should not be made available to other sites.
- Video-conferencing should be supervised appropriately for learners and customers.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use is allowed.
- Staff have access to a GSS phone where contact with customers is required. The sending of abusive or inappropriate text messages is strictly vforbidden.

Authorising Internet access

- GSS will maintain a current record of all staff who are granted Internet access.
- All staff, must adhere to GSS Internet policy before using any GSS ICT resource
- Use of GSS internet is by permission only and access to sites including but not limited to Adult content, those with extreme political or extremist views, pornography or those with any demeaning, aggressive, abusive or violent nature are strictly forbidden.

ASSESSING RISK

GSS will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a GSS computer. GSS does not accept liability for the material accessed, or any consequences of Internet access. GSS will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate

TYPES OF E-SAFTY BREACHES

- Unauthorised use of email or mobile phones
- Use of unauthorised instant messaging / social networking sites
- Accidentally or maliciosuly accessing offensive material and not notifying a member of staff.
- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Transmission of commercial or advertising material
- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or

infringes the conditions of the Data Protection Act, revised 1988

Breaches of e-safety may consist of a single act or repeated acts as above.

PROCEDURE IN THE EVENT OF A BREACH

1. This procedure must be followed whenever an allegation of e-safety breach is made or when there is a suspicion that a beach is taking place
2. Promises of confidentiality must not be given as this may conflict with the need to ensure the safety and welfare of the individual.
3. A full record shall be made as soon as possible of the nature of the allegation and any other relevant information.
4. This must include information in relation to the date, the time, the place where the alleged breach happened, your name and the names of others present, the name of the complainant and, where different, the name of those involved in the breach, the nature of the breach, a description of any concerns observed
5. For the avoidance of doubt GSS will deem any of the above perpetrated by GSS staff (including Associates, agency staff, temporary and contract) to constitute gross misconduct and as such will result in disciplinary action being taken against them.

REVIEW

This policy may be amended as and when it becomes necessary due to any significant changes in local arrangements or in statutory requirements. The policy is in conjunction with GSS GDPR policy and our Confidentiality and Privacy policy.

This policy will be reviewed on the anniversary of the date of this policy, unless otherwise required to do so.

Signed by Sonia Benjamin-Leach
Director
July 2019 v 5