Group Standard

Acceptable Use of Information Systems Including Social Media

Serco recognises its responsibility to ensure that employees access, process and publish information in accordance with Serco's social and ethical principles, legal requirements, with appropriate privacy and security, and in a manner that maintains and enhances the reputation of the company

Document Details

Document Details	Serco Business
Reference SMS GS-BC1	**Version** 7
Approval Date October 2020	**Date for next review** October 2022
Applicability Serco Group covering all business regions, operating companies and business units throughout the world[1] covering: - employees, officers, directors and individuals working as consultants and contractors and any other parties acting as representatives or agents of Serco (Employees) - wholly owned subsidiaries and majority-owned operations Where a minority interest and in regard to its subcontractors and suppliers Serco encourages alignment with this Standard	
Authority Chief Executive, Serco Group plc	
Accountable Policy Owner (Group) Chief Information Officer	
Additional Information Supporting standards, standard operating procedures and guidance relating to this Group Standard are available within the Serco Management System	
Governance Our policies and standards, together with any regional or market requirements and enhancements to them, are authorised through a robust governance process.	
Consequence Management As a Group Standard the requirements detailed in this document are mandated and must be adhered to. Non-compliance will have consequences which may include disciplinary action. The Consequence Management Group Standard (SMS-GS-G1) details how instances of non-compliance will be dealt with	

[1]As used herein, Serco Group and its affiliates, subsidiaries and operating companies are referred to as "Serco". The "Company" or "company", or "we", "us" or "our"

Contents

1 Objectives

Serco recognises its responsibility to ensure that employee's access, process and publish information in accordance with Serco's social and ethical principles, legal requirements, with appropriate privacy and security, and in a manner that maintains and enhances the reputation of the company.

Serco recognises the benefits and opportunities that social media can bring as a tool and respects all employees' right to a private life and self-expression. However, there is an inherent risk involved in using social media. It is an instantaneous and far reaching form of communication and inappropriate use can impact upon employees, the reputation of Serco, as well as its ongoing relationships with customers, which are all of vital importance to the business.

This standard sets out the behaviours that are required to be adopted, the rules that employees must abide by and the legal requirements that must be complied with when using information systems, which includes the internet, social media[1] and email (whether or not they are provided by Serco and whether or not they are used in or outside of work) to access, process and publish information either owned by or referencing Serco, our employees, clients or business partners.

All media should be assumed to be open to public scrutiny and individuals have a responsibility to consider any materials they publish or write in the light of public opinion. Individuals and managers need to be mindful that, as a private company, Serco is even more susceptible to public view and opinion than other organisations and should therefore be especially vigilant.

2 Policy Standards

2.1 General requirements

S1. Serco fully respects the legal rights of our employees in all countries in which we operate. However, activities which affect Serco's business interests (whether in or outside of work) are a proper focus for company policy.

S2. All employees will ensure that their actions and the information they access, process and publish which relate to Serco (whether in or outside of work) comply with:

a. Serco's values
b. Serco's Code of Conduct
c. relevant Serco policy standards and operating procedures
d. all applicable laws (including copyright, trademarks, the fair use of material owned by others and data protection legislation), and
e. do not result in harm or damage to Serco's reputation

S3. The loss of any device such as laptops, tablets, mobile phones, PDAs, removable media devices (i.e. USB stick, CD, memory card etc.), document or any paperwork that contains information with a Classification of 'Serco Restricted and Sensitive', will be reported to the local or regional service desk, notified to the employee's line manager and recorded as a security incident on Assure.

S4. Contracts, customers, Business Units or Divisions may have additional requirements for acceptable use over and above those detailed in this standard. Any additional requirements for the acceptable use of information systems which are applicable to your job and/or place of work must be read and understood

S5. Failure to comply with these requirements for acceptable use, may lead to disciplinary action and/or legal proceedings. Failure to comply may also result in legal proceedings against Serco

[1] Any type of interactive online media that allows parties to communicate with each other or to share data

2.2 Training and awareness

S6. New employees will be advised, and existing employees regularly reminded, of the Company's policies and requirements in regard to the acceptable use of information systems and will be provided with updates to those policies or changes in local requirements

2.3 General principles and personal use

S7. Information systems (IS) provided by Serco may be used for appropriate personal use. However, personal use should only ever be of a reasonable duration and frequency, and must not detract from your performance or that of your colleagues, harm the company's reputation or interfere with the operation of Serco's business

S8. Telephones (including mobile phones and Personal Data Assistants (PDAs) provided by Serco) may be used to make a reasonable level of personal calls.

S9. Telephones provided by Serco will not be used to make calls or send texts to premium rate numbers (unless specifically required to do so for business reasons), access non-business related subscription services or applications, or make private international calls (except when abroad on company business)

S10. No calls made or texts sent will be abusive to or harass the recipient

S11. Serco's information systems will not be used to conduct any unapproved private employment or business activities that are not related to Serco's business

S12. The use of IS will comply with all applicable laws of the country/territory in which the use takes place

S13. Serco may limit the personal use of IS where the company considers this is appropriate due to possible or actual interference with its business. Where an employee chooses to use Serco IT for personal use they do so at their own risk and Serco accepts no liability for the confidentiality or availability of any stored data. Any information will be subject to Serco policies on data handling, inspection, storage and retention.

S14. Employees who are issued with a standard Serco PC will only rebuild or change any configuration with the permission of their IS support team

S15. When an employee or contractor leaves Serco, all Serco IS, and equipment must be returned to Serco prior to the individual's departure.

S16. When an employee or contractor leaves Serco, all Serco information must be either deleted or moved to an appropriate Serco storage location prior to the individual's departure.

2.4 Use of personal equipment

S17. Serco employees and contractors may use personally owned devices such as computers, tablets and mobile phones to view Serco information stored in approved Serco IS and employees must at all times adhere to the instructions or guidance provided as part of the service

S18. Serco employees and contractors may not transfer or store Serco information to any personally owned computers, tablets, mobile phones or other devices unless the device is enrolled in either an approved Serco Mobile Device Management (MDM) service or an approved Mobile Application Management (MAM) service

S19. If an employee has enrolled a device in any approved Serco device or application management service, Serco reserves the right to review that device under special circumstances (such as a formal investigation)

S20. Personally owned computers, tablets, mobile phones or other devices may not be used for privileged access (e.g. Administrator or Root access) to Serco systems[2]

2.5 Internet

S21. IS provided by Serco will not be used to:

[2] Third party partners may use their corporately provided devices to administer Serco systems through an approved Serco Privileged User Management system

a. view, create, amend, distribute, transfer, store or print information that is pornographic, obscene, indecent, hateful, defamatory or offensive
b. engage in any form of illegal activity, including fraud, plagiarism, forgery, any form of intimidation or harassment
c. participate in online gambling, or for soliciting for personal gain or profit
d. download, store, copy or transmit the works of others (including software, games, music and video files), without their permission, where this infringes copyright or otherwise contravenes the owner or licensor's terms and conditions regarding permitted use

S22. All information created will be fair to and respect all religions, political, economic and racial differences and opinions and show proper consideration for others' privacy

S23. Employees will not commit Serco to any form of contract or obligation or enter into any IS third party contract (e.g., internet-based services, Software as a Service (SaaS) or applications) without appropriate authorisation

S24. The use of the Internet, including social media must not affect the work employees are required to perform for Serco. Should this be the case, then the company may decide to limit access to the internet and other IS for personal use

2.6 Electronic publishing – use of social media

S25. In general, Serco recognises the rights of our employees to use social media as a medium of self-expression

S26. The following standards relate to all employees in a personal capacity. They apply to all use and forms of social media where there is potential impact to Serco, whether for work-related or personal use, whether during working hours or otherwise and whether social media is accessed using Serco facilities and equipment, or equipment belonging to employees or any other third party.

S27. When using social media:

a. make it clear when publishing information associated with Serco that comments and views expressed are personal and that you are speaking on your own behalf and do not represent those of Serco (unless authorised to speak on our behalf). Write in the first person, use a personal email address and use a disclaimer such as "The postings on this site are my own and don't necessarily represent Serco's positions, strategies or opinions."
b. Any information that is published must be correct and fair, and where mistakes occur, must be corrected as soon as possible
c. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager
d. You should report any misuse by a colleague or content that is wrong, unfair or reflects poorly on us by contacting your manager, the divisional communications team or Speak Up
e. You should always be respectful to others and of their opinions and attempt to protect Serco's image, reputation, brand and identity wherever possible
f. When you leave Serco, please ensure that you update any references to your employing organisation (i.e. removing Serco as your employer from LinkedIn, etc.)

S28. You must not express opinions on our behalf or use Serco's name or logo in your social media name, handle or URL (unless expressly authorised to do so by your manager).

S29. Material which refers to Serco or uses the company's name on multi-media and social networking websites (such as Facebook, YouTube, Instagram, WhatsApp, LinkedIn, Twitter, blogs, wikis, newsgroups and any other site where text can be posted) may be published, providing that this is done in a professional and responsible manner and does not harm or tarnish the image, reputation and goodwill of Serco and our employees in a knowingly or recklessly defamatory manner

S30. Information that is false or otherwise defamatory about an individual or organisation directly connected to Serco (for example, Serco employee, customer, supplier or partner) shall not be published

S31. Do not harass, bully, threat, discriminate or be offensive or intimidating towards employees, customers, suppliers or third parties

S32. Any information that is published must be correct and fair, and where mistakes occur, must be corrected in a timely manner

S33. When publishing information related to work or subjects associated with or about Serco in a personal capacity, it must be made clear that the comments and views expressed are personal and do not represent those of Serco; a disclaimer on such comments will be used, e.g. "The postings on this site are my own and don't necessarily represent Serco's positions, strategies or opinions." Personal views or opinions must not harm the company's image and reputation

S34. Social media will not be used in a way that might breach any of our policies, any express or implied contractual obligations, legislation, or regulatory requirements. In particular, do not engage in illegal activity or engage in any activity that promotes terrorism.

S35. Information will not be published which could compromise personal security of colleagues, customers or the business. Particular care will be taken regarding government or public sector clients. Employee vetting status or the sensitivity of the work done will not be disclosed

S36. Information that is confidential or proprietary to Serco or to any third party that has disclosed information to Serco will not be published or used

S37. All requests from the company not to discuss topics for confidentiality or legal reasons will be complied with. Similarly, requests made by Serco to remove information which has been published which breaches legislation, regulations or company policies will be complied with

S38. Material will be kept up-to-date and care taken not to compromise Serco intellectual property, misrepresent Serco or communicate in a manner which may harm the image and reputation of the company

S39. If material is found on-line about Serco that is wrong, unfair, or potentially defamatory, this will be notified to line management or the Divisional communications team

2.7 Intranet

S40. Information available on Serco Group's intranet and collaboration sites (e.g. myserco and the hub) is intended solely for use by Serco. Third parties will only be permitted access to the information on the intranet where a confidentiality agreement is in place, and where there is a legitimate Serco business requirement for the third party to have access, (which will be limited to the specific information needed to fulfil the business requirement)

S41. Only information relating to Serco business will be published on its intranet

2.8 Electronic mail and messaging

S42. All employees are responsible for the content of all text, audio and images that they send using Serco's electronic mail (email) and other messaging systems (which include instant messaging and text messaging)

S43. Material that is pornographic, obscene, hateful or defamatory, or that is intended to harass or intimidate any other individual will not be sent or solicited using Serco's information systems

S44. If such material is received it must be reported to line management. The email should be retained in your inbox until advised of the appropriate course of action that should be taken

S45. Only email addresses and messaging systems supplied by Serco, our customers or partners will be used to send and receive information related to any business conducted on behalf of the Group

S46. Personal email accounts (e.g. Hotmail, Yahoo, Gmail), instant messaging and text messaging systems will not be used to transfer classified information, sensitive information owned by or relating to customers, or marked 'Serco Restricted and Sensitive' or 'Serco Business', as these are not as secure as Serco's email systems

S47. Serco's standard disclaimer, which is attached to the end of each email sent from Serco's email systems, must not be removed

S48. Email and messaging systems will not be used to generate unsolicited messages, including the sending of junk mail or other advertising material to individuals who have not specifically requested such material

S49. Spam email and messages will not be replied to or forwarded to any other individual, as they often contain malicious content or harmful links

S50. Anonymous emails will not be sent from Serco systems, nor will email and messaging systems be used to create or forward 'chain letters', 'Ponzi' or other 'pyramid' schemes of any type

S51. Vigilance should be maintained for suspicious looking email and messages, which should be deleted immediately, and the local IT department or manager informed. In case of any subsequent forensic examination the suspicious email must be retained in the deleted or recovery folder for a minimum of one month

S52. The content of email and messaging systems provided by Serco is subject to the Group standards and procedures regarding business records retention, storage and deletion[3]

S53. The automated forwarding of emails to public email services or to any third party partner or supplier is not permitted, the only exception being the automated forwarding of emails to customer systems where requested by the customer, but this is only acceptable where there is full business justification and approval has first been obtained from the divisional and business unit Data Protection Offices

S54. Serco email addresses should not be registered for any online service (i.e. a website that requires registration to create an account), unless the use of that service is business-related

2.9 Keeping information secure

2.9.1 Passwords

S55. All passwords assigned for the use of Serco information systems will be kept safe. User identity or passwords or any other access code must not be written down, displayed or disclosed to any other individual. Users must not access information with a user identity or password which is not their own

S56. If an employee has any suspicion that their password has been used by some other person, then they must change their password and report it as a security incident, in line with company procedure[4]

S57. Passwords will be created and managed in accordance with the Serco Group Security Controls Manual[5], the key requirements of which are:

a. passwords will be a minimum of 10 characters in length
b. previous passwords should not be re-used. IT systems will block the use of the previous 12 passwords
c. Different passwords should be used for different systems
d. Passwords for Serco accounts must not be re-used for personal social media, email or website accounts
e. passwords that could easily be guessed by others (i.e. birthday, children's names etc.) will not be used

S58. Should any employee be asked to disclose their password or any other access code by support personnel, they should contact their Accountable Security Manager.

S59. The digitised signature of another will not be used without their consent

2.9.2 Privacy

S60. All information will be classified in accordance with the Group Security Standard[6]

S61. It is the responsibility of the employee to ensure that their laptop is encrypted in line with company policy

S62. Information with a government classification that comes with any prescribed handling requirements or is classified as 'Serco Restricted and Sensitive' will not ordinarily be copied onto removable media, unless there is a significant and unavoidable business requirement to do so. If this information needs to be stored on USB flash drives, the device used will be approved by Serco and provided with built-in encryption

S63. Similarly, information held on other types of removable media will be encrypted using Serco approved encryption software

S64. Information with a government classification or classified as 'Serco Restricted and Sensitive' will be encrypted when transmitted by electronic means (email or file transfer) over the internet

[3] See Document Retention GSOP Ref: SMS GSOP II1-2
[4] See Incident and Fraud Reporting and Management GSOP Ref: SMS GSOP O1-2
[5] See Group Security Controls Manual, SMS-GSOP-S-GSCM
[6] See Security Group Standard Ref: SMS-GS-S1

S65. Information with a government classification, or classified as 'Serco Restricted and Sensitive' will not be disclosed to any person who does not have the right or need to know

S66. Sharing of the information classified as 'Serco Restricted and Sensitive' or 'Serco Business' with third parties requires the completion of a Non-Disclosure Agreement (NDA) with the third party prior to sharing

S67. Personal information will only be held or processed in accordance with relevant national and territory law. Unauthorised information about Serco employees will not be provided or disseminated to outside parties

S68. Personal computers (desktop and laptop) will be locked (using the Ctrl+ Alt+ Delete then Lock Computer or by activating the Sleep or Screen Saver options on Apple PCs), and documents with a government classification, or classified as 'Serco Restricted and Sensitive' must be secured when left unattended, to prevent unauthorised access

S69. To support the update of security policies and the application of software patches and updates, desktop and laptop computers will be fully shut down at least once in every 24-hour period. Desktop and laptop computers must be fully shut down when not in use for a significant period of time

S70. When taking photographs to be published either externally on social media sites or internally, staff should ensure that items in the background do not display any client information or anything which fails to meet the requirements of Section 2.6 of this document

2.9.3 Information Systems

S71. When transported in a vehicle, PCs and other IS equipment will be stored out of sight. If the vehicle is left unattended at any time, then all PCs and other IS equipment will be stored in the boot and the vehicle must be locked. For IS equipment holding any form of sensitive information an assessment must be undertaken with the local security lead as to whether a vehicle boot safe is required. PCs and other IS equipment will not be left in the vehicle if unattended for a longer period of time (i.e. overnight)

S72. IS equipment will not be left unattended in a public location (including airports, hotel lobbies, train stations, internet cafes, etc.) or on public transport, taxis, trains and planes

S73. IS equipment will not be connected to Serco or customer-owned communication networks without permission from Serco and the relevant network owner

S74. Anti-virus software, including a subscription to an update service, must be installed on any device which is used to connect to Serco, customer or third-party networks and information systems

S75. An appropriate and approved method of encryption will be deployed to prevent unauthorised access to Serco Restricted and Sensitive information held on PCs (desktop and laptop), portable devices and removable media, and when transmitted using email and other electronic file transfer systems to any third parties

S76. All Serco PCs/devices and removable media used for business purposes will have an appropriate and approved method of encryption and corporate device management, unless permanently located wholly within secure Serco premises or if the site has been approved by the Divisional Security Lead as being secure

S77. Any non-Serco PC/device or removable media that is used to store Serco Business, Serco Restricted and Sensitive or customer data will have an approved method of encryption and corporate device management, unless permanently located wholly within secure Serco premises or if the site has been approved by the Divisional Security Lead as being secure. This includes employees' personal PC/devices whether or not they are part of a Bring Your Own Device (BYOD) programme or equivalent and any PC/devices used by suppliers, consultants or contractors

S78. Malicious programmes (e.g. viruses, trojans, email bombs etc.) will not be intentionally introduced into Serco's, our partners' or our customers' information systems, unless specifically authorised to do so as part of approved security activities

S79. No employee will:

a. disrupt network communications, interfere with, harass or deny service to any other user or make changes to another IS system that renders it unusable by others
b. intentionally access or transmit information about, or software designed for, breaching security controls
c. create computer viruses or monitor or intercept network traffic, unless specifically authorised to do so as part of security activities
d. remove or disable company-installed anti-virus software and malware controls
e. attempt to crack or capture passwords or decode encrypted information

2.9.4 Information Classification

S80. If you are creating or updating a document you must classify the information as 'Serco Business' or 'Serco Restricted and Sensitive' in accordance with the Information Classification and Handling Section of the Group Security Controls Manual[7]

S81. Information classified as 'Serco Restricted and Sensitive' may be shared on virtual meeting and collaboration software

S82. Information classified as Serco Restricted and Sensitive (SRS) must be restricted on a need to know basis with only authorised Serco employees, or specified authorised external persons or entities. A non-disclosure agreement or confidentiality clause as part of a contract with all external persons or entities must have been executed prior to such disclosure and controls implemented to cover the secure distribution (e.g. ensuring the encryption of this data when at rest or in transit)

S83. Information classified as 'Serco Restricted and Sensitive' must not be published on any enterprise social networking tools (e.g. Yammer)

2.9.5 Collaborative meetings

S84. The preferred method for collaborative meetings is to use Serco-provided collaboration tools and the associated secure file storage systems

S85. Where appropriate, non-Serco employees may be invited to join Serco-hosted collaborative meetings hosted through Serco-hosted collaboration tools. Serco information may be shared, and sessions recorded through these tools

S86. Serco users may register for and join externally hosted meetings using Serco-managed equipment, provided that the meeting is accessed through the browser. Serco users may not install applications provided by externally hosted collaboration sites on Serco-managed equipment

S87. Serco users should not host meetings using external services

S88. Files must not be transferred using externally hosted collaboration sites. If the session is being recorded, recording must be suspended while any confidential or sensitive information is being viewed

2.10 Monitoring

S89. Serco is ultimately responsible for all business communications but will, as far as possible and appropriate respect the privacy of our employees whilst working

S90. Serco reserves the right to actively monitor, intercept and review, without further notice, employee activities using our IT resources and communications systems, including but not limited to social media postings or usage, in order to:

a. ensure that standards are adhered to
b. prevent unauthorised use
c. comply with legal obligations
d. prevent and detect criminal activities
e. ensure secure and effective operation

[7] See Serco Group Security Controls Manual Ref: SMS-GSOP-S-GSCM

S91. The company may review content stored on its information systems and monitor telephone, email and internet traffic data (i.e. sender, receiver, subject, attachments to emails, numbers called, and duration of calls and files downloaded from the internet) generated on its networks, including business and personal content and communications

S92. Activity conducted by the company that monitors the use of information systems will comply with the legislative requirements governing the subject

S93. Serco may use any information it receives via monitoring processes to investigate any claims of breach of this standard or any law, and to instigate appropriate disciplinary or legal proceedings

S94. Information obtained through monitoring will only be disclosed to a relevant external agency if required by law or those directing the investigation i.e. Serco management, Legal or Human Resources (HR). The information obtained will be held for as long as necessary to complete enquiries, or if part of disciplinary proceedings, in accordance with the relevant retention period

S95. Wherever reasonable, managers or HR will consult with employees about any suspected breach of this standard before any action is taken. However, this may not always be practical where illegal behaviour or gross misconduct is suspected

2.11 Remote Working

S96. When remote working (including working from home), employees must read and apply any related regional or local guidance

S97. Employees must take measures to ensure meetings and / or conversations about work can't be easily overheard. This includes not conducting conversations in public locations, using headphones where appropriate, and removing or disabling smart listening devices (such as Amazon Echo, Google Home, and Smart TVs)

S98. Employees must ensure that Serco information cannot be viewed by those without a direct 'need to know'. This includes ensuring screens cannot be overlooked, devices are either powered down (if left unattended for longer periods) or screen locked (for shorter periods), information in hardcopy is stored where it cannot be overseen or inappropriately accessed, and paper documents are shredded prior to disposal

3 Responsibilities & Accountabilities

S99. The following responsibilities will apply to the delivery of the defined standards. If these are not completed effectively, the person responsible will be accountable for any consequences[8].

Group

S100. The Group CEO will appoint a Group Information Technology (IT) Lead responsible for:

a. developing and maintaining Group Acceptable Use policy
b. ensuring standards and associated procedures and key controls remain fit for purpose, reflect legislative and regulatory requirements and effectively manage acceptable use risks
c. providing oversight and reporting acceptable use performance

Division

S101. The Divisional CEO will appoint a Divisional IT Lead responsible for:

a. implementing acceptable use policy, standards, procedures and key controls across the Division; which may include the development of country/region/Divisional procedures and management systems
b. ensuring procedures and key controls, remain fit for purpose, reflect legislative and regulatory requirements and effectively manage Acceptable Use risks
c. providing oversight of the application of this Group Standard
d. actively communicating the requirements of the Acceptable Use policy, including expected standards in the use of social media

Contract/Function

S102. The Contract Manager (or Corporate Function Head) is responsible for:

a. communicating the requirements of the Acceptable Use policy, standards, procedures and key controls

[8] See Consequence Management Group Standard Ref: SMS-GS-G1

b. ensuring all employees understand the standards of behaviour, including their use of social media, expected of them and escalating matters when behaviour falls below its requirements
c. implementing local controls for providing assurance that Acceptable Use risks are being effectively managed

All employees

S103. All employees are responsible for:

a. following defined Acceptable Use policy, standards, procedures and work instructions
b. telling a line manager of any Acceptable Use concerns or misuse of social media

4 Processes and Controls

4.1 Governance processes and controls

Process
A set of related activities that must be carried out to achieve policy outcomes

Controls
The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility
for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
P1	Acceptable Use responsibilities are defined and understood	C1	A Group Information Technology (IT) Lead is appointed by the Group CEO with responsibility for: • Developing and maintaining Group Acceptable Use policy • Ensuring standards and associated procedures and key controls remain fit for purpose, reflect legislative and regulatory requirements and effectively manage acceptable use risks • Providing oversight and reporting acceptable use performance	■	■	■	■	■

Process
A set of related activities that must be carried out to achieve policy outcomes

Controls
The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility
for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
		C2	A Divisional IT Lead is appointed by the Divisional CEO with responsibility for: • Implementing acceptable use policy, standards, procedures and key controls across the Division; which may include the development of country/region/ divisional procedures and management systems • Ensuring procedures and key controls remain fit for purpose, reflect legislative and regulatory requirements and effectively manage acceptable use risks • Providing oversight of the application of this Group Standard • actively communicating the requirements of the Acceptable Use policy, including expected standards in the use of social media	■	■	■	■	■
		C3	Contract Managers and Corporate Function Heads are responsible for: • Communicating the requirements of the Acceptable Use policy, standards, procedures and key controls	■	■	■	■	■

Process
A set of related activities that must be carried out to achieve policy outcomes

Controls
The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility
for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
			• Implementing local controls for providing assurance that Acceptable Use risks are being effectively managed					
		C4	All employees are responsible for: • Following defined Acceptable Use policy, standards, procedures and work instructions • telling a line manager of any Acceptable Use concerns or misuse of social media	■	■	■	■	■
P2	Establish policy	C5	Policy, standards and Group procedures are defined and published	■	■	■	■	■
		C6	Policy requirements for acceptable use of information systems and social media are communicated and implemented	■	■	■	■	■
P3	Establish systems and process	C7	Appropriate systems and procedures are in place to meet the requirements for acceptable use of information systems, social media and related legal requirements	■	■	■	■	■

Process
A set of related activities that must be carried out to achieve policy outcomes

Controls
The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility
for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
		C8	Systems and procedures are periodically reviewed and updated	■	■	■	■	■
		C9	Legal and regulatory requirements are monitored with changes reflected in systems and procedures	■	■	■	■	■
P4	Compliance assessment and audit	C10	A compliance plan is in place which includes assessment of acceptable use of information systems and social media	■	■	■	■	■
		C11	Compliance and audit reports have action plans to address non-conformities	■	■	■	■	■
		C12	Agreed actions are closed out	■	■	■	■	■

4.2 Key processes and controls

Process
A set of related activities that must be carried out to achieve policy outcomes

Controls
The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

Responsibility
for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S75)	Division (S76)	Business Unit	Contract (S77)	All Employees (S78)
P5	Raise awareness of policy requirements	C13	All employees have been made aware of Serco's policy and requirements around the acceptable use of information systems and social media	■	■	■	■	■
P6	Monitor use of internet, email, messaging and other information systems	C14	A procedure is in place for appropriate monitoring of the use of internet, email, messaging and other information systems and social media	■	■	■	■	■
P7	Removal of information	C15	A procedure is in place to request the removal of published information	■	■	■	■	■
P8	Manage third party access to systems	C16	Non-Disclosure/Confidentiality agreements are in place for third parties accessing Serco systems and intranet	■	■	■	■	■
P9	Manage email disclaimer	C17	The standard Serco email disclaimer is attached to the end of emails	■	■	■	■	■
P10	Manage passwords	C18	Passwords comply with password guidelines	■	■	■	■	■

Process		Controls		Responsibility				
A set of related activities that must be carried out to achieve policy outcomes		The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference		for ensuring controls are in place and operating effectively				
Ref	**Description**	**Ref**	**Description**	**Group (S75)**	**Division (S76)**	**Business Unit**	**Contract (S77)**	**All Employees (S78)**
		C19	Passwords are kept safe and not written down, displayed or disclosed to others	■	■	■	■	■
P11	Manage virus protection	C20	All devices which connect to Serco, customer or third-party networks or information systems have approved anti-virus software, including a subscription to an update service	■	■	■	■	■
P12	Encryption of PCs/devices and removable media	C21	All PCs/devices and removal media have an approved and appropriate method of encryption, unless permanently located wholly within Serco secure premises, or if the site has been approved by the Divisional Security Lead as secure	■	■	■	■	■

5 Supporting documentation and guidance

The following should be read in conjunction with this standard:

Ref	Document
SMS-GS-G1	Consequence Management Group Standard
SMS-GS-S1	Security Group Standard
SMS-GS-II1	Information and Date Management Group Standard
SMS-GSOP-II1-2	Document Retention GSOP
	Code of Conduct
SMS-GSOP-S-GSCM	Group Security Controls Manual

6 Definitions

Term	Definition
Accountability	Being accountable means being not only responsible for something but also answerable for your actions.
Responsibility	A responsible person is the individual who completes the task required. Responsibility can be shared and delegated. All responsible persons will also be accountable for completing tasks effectively. Non-compliance will have consequences which may include disciplinary action as defined within the Consequence Management Group Standard.
Group	Serco Group plc is the administrative centre of the organisation, responsible for setting corporate strategy, defining governance requirements and supporting the business in its day to day operations
Division	The Group will define a set of business divisions which will be responsible for business delivery within a defined set of markets or geographies.
Business Unit	A Business Unit is a cluster of contracts which provide a similar service e.g. Health, Defence, Transport etc. Where appropriate, a separate legal entity wholly owned or where Serco has a controlling share may also be referred to as a Business Unit, where appropriate. This may also refer to Counties/Territories
Contract	A Contract provides specified requirements to a customer (either directly with Serco or to a consortium/Joint Venture in which Serco is a party) A Contract will also refer to a corporate/functional area. Corporate/functional areas are functions which support the business and they include finance, HR, procurement etc.
Contract Manager	This refers to a manager with responsibility for managing the performance of a contract and can include a Contract Manager on a day-to-day basis (or Operational Manager with devolved responsibility), a Contract Director, Partnership Director and/or Business Unit Managing Director

Term	Definition
BYOD	Bring Your Own Device - the policy of permitting employees to bring personally owned devices (e.g. laptops, tablets, etc.) to their workplace, and use those devices to access and store privileged company or customer information and applications.
Employee	Includes all full-time and part-time employees remunerated by Serco and its subsidiaries, contractors, and consultants.
Information Systems (IS)	All IT and communication systems, equipment and media used by Serco employees (as defined above) to perform their duties and/or publish any information relating to Serco, including, but not limited to the Internet, intranet, social media, email, messaging and telephones.
Classification	Any information marked under a mandated classification scheme of the government of the country or territory of operation, customer, partner or vendor.
Remote Working	Working from anywhere except a designated Serco office. Includes working from home.
Removable Media	Refers to storage media which can be removed from its reader device, conferring portability on the data it carries, and includes Memory cards (Compact Flash card, Secure Digital card, Memory Stick), Floppy disks/Zip disks, Magnetic tapes, USB flash drives and external hard drives.
'Serco Restricted and Sensitive'	SRS information is our most valuable information, which, in the wrong hands could cause serious damage to us, our customers, shareholders, partners or suppliers through serious loss of reputation; significant financial loss; loss of opportunity; or legal action. This information may belong to the Company, customers, or third parties. Access to SRS information must be restricted on a need to know basis with only authorised Serco employees, or specified authorised external persons or entities being granted access. Encryption and controls over the distribution outside of Serco must be in place for all SRS information.
'Serco Business'	SB information is information which if disclosed without authorisation, may cause unwanted exposure of the inner workings of the company, but would not result in significant financial loss or serious harm to the company or its business interests. In essence, it is any information that is not generally made available to the public unless approved for release. This information is generally available within our offices, systems or intranet and all company employees and affiliate employees are permitted to have general access to this kind of information. This information must not be shared beyond the company premises unless with approval for formal business engagement.
Social Media	Social media is defined as a type of interactive online media that allows parties to communicate with each other or to share data. This includes online social forums such as (but not limited to) Twitter, Facebook, Instagram, Snapchat, LinkedIn and other anonymous apps, blogs, message boards, video and image sharing websites such as YouTube and Flickr.
Third Party	An individual who is not an employee of Serco or an organisation that provides labour or services to Serco.

7 Further information and support

If you require any further information or support regarding this Group Standard, or if you have any suggestions for improvement, please contact the Accountable Policy Owner (Group) or email sms@serco.com