Skills Development Scotland

Using SDS IT Equipment and Systems

Descriptor	Changes made	Date	Version
Policy first implemented	July 2017		0.1
Review no.1	J Murray tracked comments	10.08.17	0.2
Review no.2	J Sweeney	11.08.17	0.3
Review no.3	IGSIG – Statement 32 Cloud Services updated	31.10.17	2.1
Review no.4	Email and internet monitoring and GDPR compliant	05.04.18	2.2
Review no 5	MFA added and Cloud Services statement updated	04.02.19	2.3
Review no.6	Aligned with EIS partner policies presented to IGSIG	14.05.19	2.4
Review no. 7	Additional sections on MFA and using public Wi-Fi	8.08.19	2.5
Review no. 8	BYOD and Phishing update	15.11.19	2.6
Review no. 9	Final amendments from IGLG	29.11.19	2.7
Review no. 10	Final amendments from Unions	26.03.20	2.8
Review no. 11	Intune section updated	24.06.20	2.9
Review no. 12	Password policy changes and minor updates	19.05.21	3.0
Review no.13	New Collaboration section added. Passwords – Three Random Words Password Manager Working from Home Cyber Essential Plus requirements for updates and BYOD security	01.07.22	3.1

Related Policies	Back Up, Data Resilience & Disaster Recovery Policy Data Protection Policy Disciplinary Policy Employee/Board Member Code of Conduct Information Access Control Policy Physical Premises Security Policy Records Management Policy SDS Policy on the Use of Protective Markings Social Media Policy Zoom Acceptable Use Policy
Related SOPs	N/A
Related Guidance	How to Recall an Email Teams for Business Recording SDS Employee Privacy Notice
Equality Impact Assessment completed	N/A
Intended Audience	All colleagues and contractors with access to SDS IT equipment and systems
Team responsible for policy	EIS – Cyber Security
Policy owner contact details (email)	chris.knight@sds.co.uk
Policy due for review (date)	July 2023

Contents

1. Policy summary 4
2. Policy purpose and objectives 5
3. Strategic context 5
4. Definitions 5
5. Scope 7
6. Personal Data and Privacy Statement 7
7. Protecting SDS IT Systems 7
8. SDS Corporate Web Filtering Service 13
9. Software and Intellectual Property 17
10. Application Security 17
11. InTune – Mobile Device Management for Corporate Issued Devices 20
12. Colleague Owned PC and Laptops (BYOD) – Device Management 20
13. Further Guidance 23

1. Policy summary

The purpose of this document is to outline the required behaviour of colleagues, contractors, and third-party organisations, when using SDS IT equipment & systems, regardless of where those using the equipment and systems are located. This policy has been designed to protect the interests of SDS, our customers, colleagues, partners, and stakeholders. The intention is not to impose intrusive constraints that are contrary to our established culture of openness, trust, and integrity, which we recognise as essential contributors to the success of SDS.

Information security is increasingly high profile, and everyone has a responsibility for protecting information and respecting confidentiality. This policy outlines the actions which you need to take to ensure that information isn't compromised or lost and should be read in conjunction with the SDS Policy on the Use of Protective Markings and Data Protection Policy.

2. Policy purpose and objectives

Use of SDS IT equipment and systems is subject to the terms of this policy, together with the relevant policies listed in section 3 below.

For contracted and third-party organisations, any breaches of this policy will be dealt with in terms of the underlying contract or agreement and may result in termination of the contract or agreement.

3. Strategic context

As a public facing agency SDS is required to adopt Information Security practices that protect its customers, its employees and its own information and data in regard to Confidentiality, Integrity, and Availability.

SDS is committed to aligning its Information Security practices with the following guidance and standards:

- ISO 27001 Information Security Standard
- Cyber Essentials UK Government Security Standard
- Scottish Government: Cyber Resilient Scotland: strategic framework

4. Definitions

BYOD: Bring your own device – A service offered by SDS to colleagues to let them have access to corporate IT systems via a colleague owned device.

Cloud Services: The cloud is the term used for software and services that run on cloud suppliers' servers and that are accessed from the internet instead of being installed on your physical computer. EIS use a cloud service provider – currently this is Microsoft.

Cloud Storage: Method of computer data storage in which the digital data is stored in logical pools described as "in the cloud". The physical storage spans multiple servers, and the physical environment is typically owned and managed by an external hosting company.

Colleagues: All SDS employees, individuals who are seconded into SDS from another organisation or who are employed through an agency, Board members and pension trustees. Everyone involved in SDS business, including third party contractors.

Cyber Essentials: Cyber Essentials is a simple but effective Government-backed scheme that helps protect organisations, whatever their size, against a whole range of the most common cyber attacks.

External Collaboration Site: An external collaboration site/platform (whether on its own or in addition to any other functionality it may have) is one which is designed to support or facilitate access to and/or sharing (upload and/or download) such as MS Teams, Dropbox, Google Drive of information among colleagues and external third parties (including but not limited to partners and customers). In the context of this policy, it may also mean collaborative meeting and/or webinar communication tools such as GoTo Webinar, Zoom etc.

Data Protection Law: This means legal and statutory requirements relating to data protection, the processing of personal data and privacy, including but not limited to:

a. the Data Protection Act 2018;
b. the UK General Data Protection Regulation;
c. the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
d. the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union;

General Data Protection Regulation (GDPR): GDPR is the EU General Data Protection Regulation which replaced the Data Protection Act 1998 in the UK in 2018 and the equivalent legislation across the EU Member States.

Information Assets: An information asset (IA) is a body of information or data that is defined and managed as a single unit so that it can be understood, shared, protected, and used effectively to further an identified business purpose or objectives. Information assets have a recognisable and manageable value to the business, with identified content, a life cycle, and risks.

Microsoft Intune: An application that manages access to SDS corporate apps, data, and resources on mobile devices.

Mobile IT Equipment: IT devices that are designed to be portable – laptops, tablets such as iPads, mobile phones (both basic and Smartphone).

Non-Standard Software: Any IT software product or application that is not included in EIS's core Service Catalogue.

Personal Data (or 'Personal Information'): Is information held about living, identifiable data subjects, including expressions of opinion or intention about them.

Phishing and Spear Phishing: Untargeted mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website. Spear phishing is a Phishing campaign directly targeted at individuals, which uses information about employees or a company to make messages appear more persuasive and realistic.

Removable Media: Data storage devices that can be used for backup, storage, or transportation of data. Examples include, but are not limited to CD/DVDs, portable hard drives; memory cards & USB devices (memory sticks, camera, music player, mobile phone).

SDS Retention Schedule: Retention schedules are used to determine how long records should be kept.

SDS IT Equipment and Systems: Any and all equipment and/or systems issued by or on behalf of SDS or used by colleagues for the purposes of their role within SDS, including but not limited to any and all standard software provided as part of the standard SDS laptop

build Microsoft Intune, Mobile IT Equipment, Non-Standard Software, Cloud Storage and Removable Media.

Standard Software: All IT software products or applications that are included in EIS's core Service Catalogue and/or have been defined as EIS-supported.

VPN: A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

5. Scope

This policy applies to and must be complied with by all SDS employees, individuals who are seconded into SDS from another organisation or who are employed through an agency, Board members and pension trustees. Everyone involved in SDS business, including third party contractors has a responsibility to familiarise themselves and comply with this policy. Breach of this policy may be dealt with under our Disciplinary Policy and Procedure.

6. Personal Data and Privacy Statement

Whenever personal data of SDS employees is processed under activities regulated by this policy, such processing will be done in accordance with SDS Data Protection Policy (including, where relevant, the additional policies and guidance referred to in it) and our SDS Employee Privacy Notice.

7. Protecting SDS IT Systems

7.1 Password Management

Colleagues are responsible for choosing appropriate secure passwords.

- Passwords must be a minimum of 8 characters;
- Create a strong and memorable password, such as by using three random words as recommended by the National Cyber Security Centre (NCSC). Refer to guidance in Appendix 1;
- Passwords should be unique for each system;
- Passwords must be kept secret and not be disclosed or shared (Note: Apple ID passwords issued for corporate apple devices and issued before July 2021 are an exception as they need to be shared with the EIS Helpdesk);
- Passwords must NOT be saved on any login screen, do not tick 'Save Password' or 'Remember me' options if these appear. In particular this applies when you are accessing remotely from a non-SDS device;
- In the event your password is compromised (known to others), you must change your password immediately and report to EIS Helpdesk.

Your SDS account password and the Bit Locker password (laptop encryption at start-up) must be different.

The use of Password Manager software is allowed but is not part of the standard software when laptops are issued. Requests to use a password manager will follow the Non-Standard Software request process (i.e. requiring a business justification).

7.2 Accessing IT Systems and Applications

All IT systems and applications must be accessed using your own/individual login ID. Using another person's login ID or sharing your login ID is not permitted under any circumstances.

Never leave an unlocked laptop unattended. Use the Windows Lock Workstation facility (windows key+L) or logout.

You must not attempt to alter the configuration of SDS issued IT equipment in any way. This includes, but is not limited to, interfering with, or overriding, anti-virus protection, encryption or using non-standard VPN. If you require configuration changes to allow for disability adaptations, contact the EIS Helpdesk Self Service Portal. You must not swap, reallocate, or dispose of SDS IT equipment. Requests for changes should be made using the EIS Helpdesk Self Service Portal. If you require additional system administration rights related to your role in SDS a request should be submitted to the EIS Helpdesk Self Service Portal.

Laptops must be connected to the SDS network at least once a month for security updates, system patches and software upgrades. Acceptable network connections are:-

- logged on using a docking station or the EIS Corp Wi-Fi service in an SDS office;
- fully log out/shut down your laptop on a regular (preferably nightly) basis;
- remotely using home or partner Wi-Fi (Note: if your home broadband is poor, you may be required to connect at an office to get all of the updates).

7.3 Access to SDS Systems outside of UK

Colleagues
Any access from outside of the UK must be compatible with the SDS Data Protection Policy.

Contact the SDS Data Protection Officer (DPO@sds.co.uk) for guidance if accessing from outside of both the UK and the European Union (EU).

Users from Third Party Organisations
Any access from outside the European Economic Area (EEA) is prohibited.

7.4 Multi Factor Authentication

To protect SDS information and systems Multi Factor Authentication has been enabled for remote access. Multi-Factor Authentication (MFA) is best practice, which adds an extra layer of protection on top of your username and password. With MFA enabled, when you sign into an SDS service or Office 365 account, you will be prompted for your username and password (the first factor), as well as for an authentication response from your registered

MFA device (the second factor - text message, authentication app challenge, email, phone call).

When is MFA enabled?

Device	Access	MFA
SDS Laptop	Either connected to the SDS network in an office or accessing remotely using Direct Access	Not required
SDS issued mobile phone or tablet	Remote access to Intune Company Portal – Office 365	Required
Bring your own device (BYOD) enrolled in / Company Portal	Remote access to Intune Company Portal – Office 365	Required
Non-SDS issued Laptop such as a home PC	Remote Access to SDS IT systems and applications and corporate Office 365	Required

When you enrol into the MFA service you can choose the authentication method that is best for you. If your choice becomes compromised or unavailable, report this to the EIS Helpdesk immediately. For example, you have chosen to receive text messages to your mobile phone and then the phone is lost or stolen, the password used to access the email account you use for MFA is compromised.

7.5 Personal Usage

Use of SDS IT equipment and systems, licences and software are provided primarily to allow colleagues to conduct their day-to-day business. Limited, occasional, or incidental use for personal purposes is understandable and acceptable.

All personal use of SDS IT equipment and systems, licences and software should be conducted in a manner commensurate with all the provisions of this policy.

In utilising systems, such as email, chat, instant messaging, and the internet, for personal purposes colleagues should have no expectation that their use is private, anonymous, or undetectable by SDS or indeed by outside agencies (see Section 7.8 below for more information on the monitoring which may be undertaken of the use of SDS IT equipment and systems).

Personal usage must therefore not:

- interfere with the performance of your work;
- take priority over your work responsibilities;
- incur unwarranted expense on SDS;
- have a negative impact on SDS in any way; or
- be unlawful or infringe the provisions of this policy or any of our other policies.

In exceptional circumstances Colleagues may request increased / frequent personal use. Requests must be approved by your People Manager and EIS must be made aware of the

requirement by logging a non-standard request on the EIS Help Desk Self Service Portal. Where personal use exceeds business use you may be subject to benefit in kind taxation.

7.6 Removable Media Usage

Only authorised USB memory sticks supplied by EIS Helpdesk may be used with SDS IT equipment. When connected to a laptop the memory stick is encrypted with 'Bit Locker to go' encryption. No SDS data/information is to be held on unencrypted memory sticks.

Removable Media should not be used to store master versions of data/information. It should be used to store copy versions only. Master copies must always be stored on the corporate systems. Limit the volume of data/information on the removeable media to the minimum required.

Delete data/information from the Removable Media held when no longer required.

For CDs/DVDs these must be destroyed by shredding or cutting them in half, when no longer needed.

For memory sticks, data/information should be deleted by formatting in such a way that the data/information cannot be recovered. If the device is to be physically destroyed or sent for secure destruction, contact the EIS helpdesk for further details. Guidance on management of memory sticks will be provided by EIS at the time of issue.

If the data/information stored on the Removable Media pertains to identifiable individuals (and therefore constitutes personal data) then you must comply with the SDS Data Protection Policy (as amended from time to time).

7.7 Information on SDS's IT Equipment and Systems Policy

SDS's information and data must always be handled in accordance with the SDS Policy on Use of Protective Markings and Data Protection Policy. It should be stored and retained in accordance with SDS's Retention Schedule. Colleagues must protect and be vigilant against accidental or deliberate compromise of SDS information, by ensuring that they meet the obligations and standards set out in this policy.

Any deliberate, unauthorised entry to systems (hacking), entry of false data and unauthorised changes to information outwith organisational processes, are strictly forbidden and could result in disciplinary action and criminal prosecution.

You must not create, view, access, transmit or download any of the following material on SDS IT equipment or systems:

- Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- Offensive, obscene, or criminal material or material which is liable to cause embarrassment to or be detrimental to the reputation of SDS or to its clients;
- A false and defamatory statement about any person or organisation;
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others;

- Confidential information about SDS or any of Colleagues or clients (except to the extent that you have authority to access same);
- Any other statement which is likely to create any liability (whether criminal or civil, and whether for you or SDS);
- Material which infringes copyright or any other third-party intellectual property rights;
- Online gambling; or
- Chain letters.

7.8 Monitoring

7.8.1 Electronic Communications Monitoring

EIS on behalf of SDS, monitors and reviews usage of all our systems, including logs of when SDS laptops and other IT equipment are logged into by each user. Any monitoring is not designed to intrude upon Colleagues' personal lives and is only carried out to the extent permitted or as required by law, and as necessary and justifiable for business purposes, based on one of these specific justifications:-

- to investigate or detect the unauthorised use of the systems;
- to ensure that the system is working effectively;
- to ensure that SDS policies, procedures, standards of work and behaviour and
- contracts are being observed;
- to assist in the investigation of alleged wrongdoing or poor performance;
- to maintain the security of SDS IT Systems and Equipment;
- for training and monitoring of standards of service;
- to detect any malicious code such as viruses or other malware;
- to provide evidence of business activities;
- to check mailboxes of absent Colleagues; and
- to comply with any legal obligation.

The specific legal basis of any processing of personal data through electronic communications monitoring (for the above stated purposes) under the UK GDPR (General Data Protection Regulation) is Article 6(1)(f): 'processing is necessary for the purposes of the legitimate interests pursued by the controller'. This has been concluded in line with the Employment Practices Code provided by the Information Commissioner's Office.

Any monitoring will be carried out in accordance with audited, controlled internal processes and the relevant legislation in force from time to time including as applicable the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000, the Data Protection Act 2018, UK GDPR, the Investigatory Powers Act 2016, and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations 2018.

7.8.2 Hardware Asset Monitoring

SDS is required to record and track all of the organisation's IT assets. To facilitate this requirement, EIS installs asset management software on all laptops. This software scans your computer and tells EIS what hardware you have as well as how it is configured. In terms of data and software the application identifies certain file types which could potentially

infringe policy, for example music files and tells EIS what software you have installed and how often this software is used.
Usage information gathered will be used by EIS to ensure the most effective use of existing assets. This may involve the removal and redistribution of under-utilised hardware and software.

7.8.3 Outlook, Email, Chat, Text Messaging, and Instant Messaging (IM) Monitoring

Emails, chats, texts and IMs (Instant Messaging) will be monitored in the first instance on the basis of the traffic record. However, occasions may arise where the contents of messages will be accessed by SDS. Any monitoring of actual content will, as far as possible, be strictly limited, targeted and only conducted where one of the justifications outlined in section 7.8 applies. In assessing whether monitoring of content is justified we will take account of the privacy of those sending emails, texts, chats and IMs as well as the privacy and autonomy of those receiving them.

In using the system for personal purposes, colleagues can mark emails as personal if they wish and the contents of these messages will not normally be accessed by SDS, except in exceptional circumstances where we have a reasonable belief that they demonstrate wrongdoing or the monitoring is otherwise necessary for a legitimate business purpose listed as specific justification in section 7.8, and it is not reasonably possible for us to obtain such information in a less intrusive manner.

A non-intrusive automated monitoring and detection process will be used to monitor the content of incoming and outgoing emails. This will detect computer viruses, spam mail or content which would infringe the terms of the Policy.

Where it is necessary to check the mailboxes of colleagues in their absence, the purpose of such monitoring will be to ensure the business responds properly to its customers and other contacts.

As part of our monitoring, if rendered necessary for one of the justifications in section 7.8, SDS may access your online Outlook work diary.

7.8.4 Internet Monitoring

Colleagues should be aware that usage of the internet is controlled and monitored (as outlined in section 7.8).

Device	Monitoring
SDS issued Laptop	All internet activity is monitored, logged and managed via the Corporate web filtering service.
SDS issued iPad or Smartphone – enrolled with Intune	When connected to the SDS Guest Wi-Fi - All internet activity is monitored, logged and managed via the Corporate web filtering service. When connected via a GSM 3/4/5G connection - All internet activity is monitored, logged and managed by the service provider. This information can be made available to SDS if requested. When connected to public or home Wi-Fi – No corporate monitoring but may be monitored by the provider.

Bring your own device (BYOD) enrolled in Intune	When connected to the SDS Guest Wi-Fi - All internet activity is monitored, logged and managed via the Corporate web filtering service. Other than using the SDS Guest Wi-Fi there is no SDS monitoring of internet access.

8. SDS Corporate Web Filtering Service

An automated web-filtering system designed to prevent unacceptable website access is in operation. This is updated daily to ensure a constant level of protection. The system helps protect and prevent colleagues from accessing sites which would be deemed to infringe the terms of this policy.

Periodically SDS will review this log to ensure that the provisions of the policy are maintained, which will include checking which pages have been visited and searches made, to the extent reasonably necessary in the interests of the business for one of the reasons outlined in section 7.8 applies. In dealing with a suspected or identifiable case of misuse, measures will be taken to protect the privacy of the colleague in terms of the sites visited. However, this will depend on the circumstances of the misuse.

Unintentional access is of course an accepted eventuality of internet access and will be considered in any subsequent investigation. By its nature it should be evidenced as extremely short access times.

8.1 SDS Issued Mobile IT Equipment

8.1.1 Mobile Equipment

- Provision of mobile IT equipment to non-employed workers is strictly limited.
- All SDS issued mobile equipment must be protected from unauthorised access and the data must be encrypted.

Device	Protection	Your Responsibility
Laptops	All SDS issued laptops have 'Bit Locker' encryption enabled. A password to unlock the device will be given to you when you receive the device.	You must protect the password you are given and not keep a note of it with the device. If you forget the password, you must contact the EIS Helpdesk. If you believe the password has been compromised, or the device is lost or stolen, you must report this to the EIS Helpdesk immediately as a matter of urgency. See Section 13 for details on reporting security incidents. Select a strong Bit Locker password – must be unique and aligned to section 7.1

iPad and Smartphones	Mandatory pin code to unlock the device and enable encryption.	When you receive the device, you will be given instructions on setting the pin code. If you believe the pin code has been compromised, or the device is lost or stolen, you must report this to the EIS Helpdesk immediately as a matter of urgency. Additional security such as fingerprints are encouraged. See Section 13 for details on reporting security incidents.

You are required to discuss with your People Manager the return of all Mobile IT Equipment when:-

- the device is no longer required;
- you are going on planned leave greater than three months; or
- if you leave the employment of SDS.

People Managers are required to complete a leavers form on the SDS Intranet which includes arrangements for returned mobile IT equipment to be picked up by EIS.

SDS has the right, at any time, to access, remotely wipe or deny user access to SDS issued mobile IT equipment in order to reduce any perceived risks. This can include deleting any personal files that you may have stored on the device (including photos, emails, and documents). Access is to the extent covered by section 7.8.1 Electronic Communications Monitoring. This does not include files that are accessed in Cloud Storage, e.g. a master document on a SharePoint site.

You have responsibility for the care of mobile IT equipment allocated to you and must take reasonable measures to ensure that it is protected from physical damage, loss and theft. For example, never leave mobile IT equipment unattended while in transit (car, airplane, train, taxi, bus etc). Furthermore, never leave it lying on a car seat and be aware that locking it in the boot also carries a risk. If in doubt, take it with you.

If you lose any mobile IT equipment, then you must report that immediately to the EIS Helpdesk. Where personal data is stored on the equipment, you must describe the personal data that is stored on the equipment as part of your report to the Helpdesk, so that the Helpdesk can then contact the SDS Data Protection Team for support if necessary.

Colleagues should take care when using mobile IT equipment in public places. You need to be aware of the increased risk of theft, of being overlooked or being overheard. You must not process highly sensitive information in public places (e.g. on public transport) where it might be heard or viewed by others.

Data stored on mobile IT equipment must be the minimum necessary to achieve the business purpose and must not be the only copy or master copy of the data. You must ensure that data stored on the device is removed when no longer required.

You must ensure that unauthorised persons do not have access to, or use, SDS mobile IT equipment. If you believe the security of a device (or any system/account) has been compromised or is at increased risk of being compromised, or the device is lost or stolen, you must report this to the EIS Helpdesk immediately and complete the Lost/Stolen Incident Form as a matter of urgency. See section 13 for details on reporting security incidents.

Non-Standard mobile IT equipment may be requested to support colleagues with disabilities. Requests should be sent to the EIS Helpdesk with approval from your People Manager.

8.1.2 Using Public Wi-Fi

Make sure you are connecting to a trusted Wi-Fi hotspot, operated by the venue. Check hotel guides or conference packs for correct public Wi-Fi name and password, and if in doubt ask a member of staff to confirm. (Note: It is possible for criminals to setup a rogue hotspot with a genuine network name or something very similar to attempt to steal your data.) If possible, you should connect using your mobile device network as a hotspot.

For SDS laptops much of the security is automatically deployed every time you login. The Direct Access software encrypts network traffic over a public Wi-Fi. For iPads and smartphones, you must use the Intune application to secure your device and to encrypt data across the public Wi-Fi network. Once Intune is installed on your device you should only use the Company Portal apps to access SDS data (OneDrive, Outlook, SharePoint). If you need internet browser access, download and use the Secure Browser app from the company portal/Intune.

If using the browser, only use sites that encrypt data over the networks - look out for HTTPS in the URL, a padlock or in Chrome the word Secure next to the URL.

Always log out of any website or service you have visited once finished.

Avoid accessing confidential or personal information.

If you notice anything suspicious about the connection on your laptop contact the EIS Self Service Helpdesk immediately.

8.1.3 Laptop Security (requirements are dependent on location)

When working at a desk within an SDS Office environment

- Access to your laptop must be locked if left unattended. Use the Windows Lock Workstation facility (windows key+L) or logout.
- At the end of your business day, the preferred option is to take the laptop with you as it will be available if a Business Continuity event makes your work base unavailable. Alternatively secure safely in a lockable area where available. Laptops should not be left on desks overnight.

In meeting rooms, touchdown and café areas using Wi-Fi

- Additional care needs to be taken to avoid a visitor gaining unauthorised access to SDS information by over-looking you when working.
- It is your responsibility to ensure any SDS issued mobile IT equipment or

confidential and sensitive materials are never left unattended and secured safely when not in use. This prevents theft, accidental damage and misuse.

When working out with an SDS secured office (including public access locations and schools)

- Laptops should not be left unattended, especially in a public place. Ensure that access to your laptop is locked (Windows key and L). Never leave laptops lying on a car seat and be aware that locking it in the boot also carries a risk. If in doubt, take it with you.

When working from home

- Use your SDS issued laptop to access SDS systems using your home Wi-Fi;
- Secure your laptop in a location to limit potential unauthorised access;
- Ensure you fully shut down your laptop at the end of each day. This is necessary for the installation of updates into the operating system and other applications; and
- Where access is restricted due to poor broadband you are required to connect your laptop in an office at least monthly to get security updates.

8.1.4 iPad Security

To access SDS information corporate iPads must be enrolled into Microsoft Intune. SDS's information should be stored on SDS systems, and in accordance with the SDS Policy on the Use of Protective Markings. Corporate iPads must be locked away when NOT in use, e.g., overnight, in a secure place.

An Apple ID, based on the colleague's email address, will be created by EIS for managing the device and downloading standard corporate apps. EIS will inform you of the password. If you change this password, then you must inform the EIS Mobility Team of the new password as this is required to enable EIS to support the device. This applies to devices issued before July 2021.

You may use a personal Apple ID on the device to access your personal iCloud storage and Apps but should be aware that App updates can only be installed with the Apple ID used to install them and you should regularly use the EIS issued Apple ID to update your device. For devices issued after July 2021 the user will have completed their own set up and passwords are not shared with EIS.

8.1.5 SDS Issued Smartphones Security

Colleagues may make personal calls. These calls must be compliant with the requirements on Personal Usage in section 7.5 of this policy. Personal calls in excess of the acceptable personal usage statement should be reimbursed to SDS via the expenses system.

SDS does not allow Smartphones to be used while driving. SDS will not provide car kits.

All SDS issued Smartphones must be enrolled in Intune.

You must ensure that:

- the phone is protected by a pin, password or biometric (Face recognition, fingerprint). Any pin or password must not be easily guessed;
- the device and applications are kept up to date;
- when you leave SDS or no longer require the mobile phone it should be restored to factory settings, then returned to EIS. How to restore factory settings; and
- when returning phones, recorded delivery or sign for courier must be used. Contact the EIS Helpdesk for the return address.

9. Software and Intellectual Property

SDS license the use of computer software from a variety of companies. We do not own this software or its related documentation. Unless authorised by the licensor, SDS does not have the right to reproduce, with an exception for backup purposes, subject to the terms of the licence. The copying of software beyond what is allowed by the licence, failure to comply with licensing terms or use of unlicensed software, can be in breach of legislation and expose you and SDS to civil and criminal liability under the laws governing software use.

9.1 Software on Laptops and Servers

Colleagues must not purchase, download or install software onto SDS laptops and servers. This includes cloud-based software applications. Requests for non-standard software will follow the Non-Standard Software request process via the EIS Helpdesk Self Service Portal.

All laptops and server software, including that downloaded from the Internet, must only be installed by designated EIS colleagues or authorised partners. All licences and media will be held in secure storage by EIS.

You must not install, copy or store on SDS laptops and systems any free or evaluation software, games, non-standard screensavers, non-business-related media files, and music files (including, but not limited to, MP3, MP4, WMA etc). Where these types of files are discovered by SDS's monitoring system they may be removed without your consent.

Non-standard specialist software may be requested to support colleagues with disabilities. Requests must be made via the EIS Helpdesk Self Service Portal.

Colleagues with SDS issued iPads and Smartphones may purchase, download, install and use applications and services from the official device Apps store. Third-party sites and alternative App stores must not be used.

10. Application Security

10.1 SDS Provided Applications (e.g. Office 365, CIAG Portal, FIPS, CSS, Agresso)

Colleagues should always use the SDS provided application and should only ever use third party supplied applications where it is not possible to use the SDS provided application.

Cloud based applications allow for access outside of SDS offices and on non-SDS issued equipment. Further care needs to be taken when accessing from a non-SDS issued device. Details are provided in section 12 (BYOD):-

- only access from a trusted device with up-to-date patching and functioning and current anti-virus software;
- never tick the save password box;
- always use the 'Logout' function to close your session;
- always close the browser after access;
- never download and save SDS documents and data onto the device;
- do not allow any unauthorised use of your SDS cloud facilities as you may be held liable for any breach of policy subsequently incurred; and
- where a cloud service provides multi factor authentication this should be used.

Care must be taken when using the SDS email service as email is the most common way that an organisation is attacked.

Colleagues should report any suspicious emails using the 'Report Message' button in Outlook. When accessing shared mailboxes, colleagues should report suspicious emails to the HelpDesk. If you do interact, specifically by, clicking on a link, entering your log in details or opening an attachment this must be immediately reported to the EIS Help Desk.

EIS regularly perform phishing tests using fake phishing templates. These tests are carried out to understand what our vulnerability would be if a real phishing attack were to happen and to raise awareness.

Take care as emails can be spoofed to appear to be from someone you know, may contain malware or could be used as part of a scam (Phishing or Spear Phishing).

Colleagues must use their SDS email accounts (@sds.co.uk) for SDS business.

Never automatically forward SDS email to a non-business email account.

Colleagues must adhere to the SDS Policy on the Use of Protective Markings and Data Protection Policy when sending data/information via email.

Colleagues should be aware that a name typed at the end of an email is a signature in the same way as a name written at the end of a letter. You may be agreeing to terms, entering a contractual commitment or making representations by email unless the appropriate authority has been obtained.

Email and instant messaging messages may be disclosed in legal proceedings, in response to a request for information under the Freedom of Information (Scotland) Act 2002 or in response to a Subject Access Request under Data Protection legislation. Deletion from a user's inbox or archives does not mean that an email or instant message cannot be recovered for the purposes of disclosure. All email and instant messages should be treated as potentially retrievable, either from the main server or using specialist software.

It is your responsibility to ensure that your emails are sent to the correct recipient and the correct attachments and links are included where relevant. You should double check recipients, email content and attachments before sending. An email sent to the incorrect

recipient, or including the incorrect content/attachments, such that personal data or confidential information is compromised, could amount to a breach of SDS's legal obligations. This may need to be reported to a regulatory body such as the Information Commissioner's Office and may be potentially damaging to SDS's reputation. If you send or become aware of such an email sent by someone else, you must report this immediately to the SDS Data Protection Officer (DPO@sds.co.uk).

10.2 Use of non-SDS provided application, cloud services and collaboration sites

Colleagues must take care when using applications and services that are not formally approved by SDS for business purposes. These services will be unsupported.

Your use for SDS business purposes must comply with the policies referenced in the cover page Related Policies section of this policy.

Prior to using Non-Standard Software, Cloud Services and collaboration services:-

- check to confirm if an alternative SDS provided tool or service is available;
- check the licensing agreements to ensure compliance. Many web applications are free for 'personal' use but require a paid for subscription for 'business' use;
- read the privacy statements to understand where data is stored and who it is shared with, and ensure this is in accordance with the Data Protection Policy;
- check the cookie policy to see what usage data is collected; and
- where a cloud service provides multi factor authentication, this should be used.

When sharing, accessing, uploading or downloading data/information, this must be carried out in accordance with the SDS Policy on the Use of Protective Markings and Data Protection Policy.

10.3 Non-Standard Software Installs

Requests for non-standard software will follow the Non-Standard Software request process via the EIS Helpdesk Self Service Portal and will require EIS Security Team review and approval as well as the Digital Assurance Group approval.

The requestor is responsible for ensuring that any requested software is kept up-to-date, and all security patches are installed within 14 days of notification.

10.4 Third Party Webmail

Access to third-party webmail services such as Gmail and Hotmail are restricted to reduce the risk of unauthorised disclosure of SDS information. If you have a business need to access these services, contact the EIS Helpdesk Self Service Portal.

Access to third-party external storage sites such as Dropbox are restricted to reduce the risk of unauthorised disclosure of SDS information.

If you have a business need to access these services, you must ensure you comply with the SDS Policy on the Use of Protective Markings and process. For requests to access these services on a short-term basis, you will be asked to read and comply with the Acceptable

Use Policy for Online Storage Access Requests. This should be completed before submitting a request to the EIS Help Desk Self-service Portal.

Guidance on using third party Collaboration sites for video conferencing and webinars is available on Connect.

11. InTune – Mobile Device Management for Corporate Issued Devices

Colleagues shall not change any pre-set Intune configurations without the permission of EIS.

Colleagues may save or copy limited data from the Intune application environment to the device:

Type of Information	Allowed outside of Intune	Example
Public information	Allowed	Presentations, brochures
Internal	Allowed	Meeting minutes, draft documents you are working on
Confidential	Try to avoid – keep to a minimum – delete when no longer required	Company data, financial information
Confidential - Sensitive	Not allowed	HR records, documents with sensitive information

Colleagues are able to install and register the Intune application on their personal mobile devices and home PCs (BYOD) for secure access to corporate applications.

SDS does not reimburse colleagues for any additional charges or cost incurred by the use of the SDS Intune service.

SDS does not provide any insurance cover for colleagues who opt to use their own BYOD personal devices.

12. Colleague Owned PC and Laptops (BYOD) – Device Management

SDS operates under Cyber Essentials. The scope for Cyber Essentials includes all equipment that contains or can access business data including devices owned by Colleagues. Therefore, all colleague-owned devices must meet the same security requirements as company owned and managed devices.

You are only permitted to access business data if your own device meets the following requirements:-

- all operating systems, firmware and applications on your own devices must be supported by a supplier that produces regular fixes for any security problems.

They must never be end of life and unsupported;

- all high-risk or critical security updates for operating systems, firmware and application on your own devices must be installed within 14 days of release;
- all software on your own devices must be licensed in accordance with the publisher's licensing terms and technical recommendations; and.
- anti-malware must be installed on your devices and set to auto update, scan files automatically upon access and scan web pages you visit and warn of malicious content.

12.1 Using SDS Intune Service (BYOD)

Colleagues who install the Microsoft Intune application on to their personal devices:

- must own the personal device;
- do so with the clear understanding that the application and contents are the sole property of SDS provided for the purpose of delivering authorised services only;
- take full responsibility for the installation and support of the application on personal devices. SDS is in no way responsible for the installation or any damage to software and hardware on the personal devices;
- must ensure that their personal device has the latest version of operating system software as recommended by the manufacturer before installing the application. Subsequent future device updates must also be maintained on the personal device to allow continued use;
- must not connect devices that are out-of-support from the manufacturer and are no longer receiving security updates;
- are licensed to install and operate the Microsoft Intune application on up to five devices;
- shall report to the EIS Helpdesk as soon as possible when a personal device with the Microsoft Intune application installed upon it has been lost or stolen, or if the security has been compromised (Examples: breach of confidentiality, compromised passwords, anti-virus alerts/warnings). Where personal data is stored on the BYOD device then this must also be treated as a personal data breach for the purposes of the SDS Data Protection Policy and reported as such immediately to the Data Protection Officer;
- must not change any pre-set Microsoft Intune configurations or profiles on the device without permission;
- grants SDS and EIS the right at any time to access, remotely wipe or deny user access to the Microsoft Intune application from the personal device in order to reduce any perceived risks;
- must ensure they do not allow any unauthorised persons to access and use features provided by the Microsoft Intune application. Doing so constitutes a breach of this policy;
- shall not use Microsoft Intune for personal use;
- must not connect to the Microsoft Intune services or install the application on devices that have been modified in ways not designed or intended by the manufacturer;
- shall not attach personal devices to SDS internal Wi-Fi network;

- should be aware that personal data held on the device outside of Microsoft Intune is their responsibility and they should take appropriate security measures to protect it;
- when not in use Microsoft Intune must be securely locked with a complex password compliant as set out in section 7.1.

All colleagues are reminded that all other relevant policies still apply when using Microsoft Intune on personal devices. A list of policies is referenced in the cover page Related Policies section of this policy.

If the colleague plans to decommission the device, no longer requires access or leaves the employment of SDS, the Colleague must contact the EIS Helpdesk to enable the remote wiping of Microsoft Intune and contents.

The Microsoft Intune configuration does not allow colleagues to save or copy SDS information outside of Microsoft Intune.

If you believe the security of your device (or any system/account) has been compromised or is at increased risk of being compromised or the device is lost or stolen, and as a result there is a risk to the security of data relating to SDS, its customers, suppliers or personnel, you must report this to the EIS Helpdesk and report using the Lost It Report It process immediately as a matter of urgency. SDS may take all reasonable steps to ensure (or minimise the risk to) the security of its data held on such device. See Section 13 for details on reporting security incidents.

SDS will not monitor or log activity on the device outside of the Microsoft Intune environment. However, it is expected that colleagues will ensure that anything they do on the device is legal and would not lead to damage to the reputation of SDS. Further guidance on expected behaviour for SDS employees can be found within the SDS Code of Conduct Policy.

13. Further Guidance

Security Incident	Reporting Process
Lost or stolen SDS issued Smartphone	**Report to the EIS Helpdesk: +44(0)300 013 2111**
Lost or stolen SDS issued mobile equipment	
Lost or stolen removable media	
Compromised data or information (hard or soft copy)/breach of confidentiality	
Lost or stolen personal IT equipment with Microsoft Intune	
Anti-virus alerts/laptop exhibiting abnormal behaviour	
Compromised passwords	
Interaction with a Phishing Email	
Unauthorised access to or loss of personal information or data	**Report immediately to the Data Protection Officer (DPO@sds.co.uk), who may require to report (within 72 hours) to the Information Commissioner's Office**

Appendix 1

National Cyber Security Centre (NCSC) guidance on Three Random Words.

- Use three random words to create a strong password.

- An effective way to create a strong and memorable password is to use three random words. Numbers and symbols can still be used if needed, for example 3redhousemonkeys27!

- Be creative and use words memorable to you, so that people can't guess your password.

- Your social media accounts can give away vital clues about yourself so don't use words such as your child's name or favourite sports team which are easy for people to guess.

- Cyber criminals are very smart and know many of the simple substitutions we use such as 'Pa55word!" which utilises symbols to replace letters.

- Never use the following personal details for your password:

    - Current partner's name
    - Child's name
    - Other family members' name
    - Pet's name
    - Place of birth
    - Favourite holiday
    - Something related to your favourite sports team