INFORMATION CLASSIFICATION and HANDLING POLICY

Approved by:	Senior Information Risk Owner
Latest Approval Date:	6 October 2021
Next Review Date:	6 October 2023
Contact:	Records Management Team

Contents

GLOSSARY

Colleagues - All staff, non-employed workers, secondees, board members, pension trustees, together with other individuals who may work with or on behalf of SE from time to time.

EIR - Environmental Information (Scotland) Regulations 2004, which provides public access to environmental information held by public authorities.

External Collaboration Sites - In the context of this policy, 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 team discussions, task planning, and access to and/or sharing (upload, download and/or editing) of information among Colleagues and external third parties (including but not limited to partners and customers).

External File Sharing Sites - In the context of this policy, an external file sharing 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) of information among Colleagues and external third parties (including but not limited to partners and customers).

External File Sharing and External Collaboration Sites should not be confused with collaborative meeting or webinar communication tools such as GoTo Webinar, Zoom etc.

FoI - the Freedom of Information (Scotland) Act 2002, which gives individuals the right to access information from public sector organisations.

DPIGO - Data Protection and Information Governance Officer is the appointed role responsible for SE's compliance with legislation, policies, procedures and guidelines relating to data protection and information governance.

Information Assets - A collection of information (hard and/or soft copy), defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently, eg Company information, grants and claims records, HR data, Board papers etc. Information assets have recognisable and manageable value, risk, content and lifecycles.

Information Asset Owners - Forms part of the role of existing senior responsible individuals who will provide advice and assurances on Information Assets in their business area to the senior information risk owner. They are able to understand and address risks to this information and ensure that information is fully used within the law for the public good.

SAR - Subject Access Request. A SAR is a request made by or on behalf of an individual for the information which they are entitled to ask for under Article 15 of the UK General Data Protection Regulation.

1. INTRODUCTION/PURPOSE

Information is a key asset and fundamental to everything that SE does. The nature of SE's activities requires Colleagues, from time to time, to share and/or access information, for the purposes of knowledge building and collaboration internally and externally of SE.

SE must be trusted by its partners and customers as an organisation which respects any information shared with us. Information classification is used to ensure that information assets are appropriately protected and handled and that information shared and/or accessed is done so in accordance with proper governance, to minimise the risk of information loss and/or data breaches.

The SE Information Classification and Handling policy therefore sets out:-

- the information classification system, with a view to ensuring that SE's information and data in, whatever form, wherever it is stored and shared, is valued and managed appropriately by the organisation, Colleagues, its partners and any other third parties; and
- SE's requirements and expectations in situations where Colleagues are involved in information storing, sharing and handling, specifying what action should be taken to minimise the related risks.

It is the **responsibility of Colleagues to ensure appropriate contractual terms or data sharing agreements are in place with third parties, when sharing, accessing or where those third parties are engaged to hold or create information on behalf of the organisation.** Information/records management and security arrangements must also be in line with our policies and procedures.

Where applicable, it is the responsibility of Colleagues to complete a Data Protection Impact Assessment (DPIA) where the information being shared comprises personal data.

2. SCOPE

This policy **applies to all Colleagues**.

Any Colleague found to have breached this policy may be subject to disciplinary or legal action. Where third parties are involved, a breach of this policy may also constitute a breach of contract.

It **covers all information assets** including:-

- Electronic documents and data, including, but not limited to, databases, records, reports, marketing and/or training materials, emails and online Chats such as those in MS Teams, Zoom, webinars and other online channels.
- Hardcopy - printed materials, including but not limited to, any of the electronic document categories listed above.
- Recordings of verbal conversations and meetings in person, by phone, voicemail etc.
- Multimedia - photos, videos, podcasts, webinars, including recordings of webinars.
- Social media postings.

From **whatever source** including:-

- SE
- Customers
- Partners
- Stakeholders
- Suppliers
- Investors.

3. KEY PRINCIPLES

- **All information is valuable and should always be treated with care** irrespective of your working location (eg home, shared workspace, public area, SE office).
- **Confidentiality must be objectively assessed and maintained** in line with the nature of the information.
- **SE must comply with statutory regulations** which include: Data Protection Act 2018, UK General Data Protection Regulation, Public Records Scotland Act 2011, EIR, FoI, INSPIRE (Scotland) Regulations 2009 and the Re-use of Public Sector Information Regulations 2015.
- **SE must maintain the trust of those that it works, partners and collaborates with** so they have confidence to share information with us or to enable us to access their information.
- **Information must only be shared with Colleagues and third parties who have a business need to see it**. The sharing of personal data or confidential information with third parties must be supported by a Data Sharing Agreement or appropriate agreement. Seek appropriate advice from Legal Services or DPIGO.

- **Only store information on authorised IT systems.** Information on equipment hard drives or removable media such as USB keys may be used for temporary storage only and are not to be used for permanent storage. These are not backed up and are more vulnerable to corruption, loss and unauthorised access if the equipment is mislaid or stolen.
- **Do not use a non-SE email address to send or receive SE Information Assets, communications, documents and other media.**
- **In the office, sensitive/confidential information must be locked away when not in use**, following SE's Clear Desk Requirements.
- **When working from home, take all necessary steps to keep private and confidential material secure** in a locked drawer or a private space (area/drawer/cupboard not visible by others inside or outside your home). Do not leave lying openly accessible in public areas.
- **Do not discuss sensitive/confidential issues in person or on the phone where you can be overheard** by third parties such as in public places, on public transport. You should also disable any listening devices, for example Alexa, Google Assist, Siri etc, if they are within earshot when you are on a confidential call at home.

Reporting Information Security Incidents

- **Report stolen, lost or potentially lost information/SE devices as soon as possible**, following the Lost It, Report It procedure.
- Any **incident which involves compromise, inability to access, unauthorised access and/or disclosure of Information Assets must be reported as soon as possible**, following the Lost It, Report It procedure.

4. HOW TO IDENTIFY AND LABEL INFORMATION ASSETS WITH AN APPROPRIATE CLASSIFICATION

Information Classification Definitions

Label	Definition
Public	Information that has been made publicly available via SE's websites, other public media channels and/or under a FoI request.
Internal	The majority of information processed by Colleagues which, if disclosed, particularly outside SE, would be inappropriate. This classification need not be marked on the document.
Confidential	Information that SE holds and is SE, company confidential, subject to a non-disclosure/confidentiality agreement, and/or personal data, the unauthorised disclosure of which, even within SE would cause or has the potential to cause significant harm to the interests of SE or other parties.
Confidential Sensitive	This is a sub-classification of Confidential and may be applied to information where loss or disclosure would have damaging consequences for SE or causes significant damage or distress for an individual or group of people, eg sensitive information such as organisational restructuring, special category data* or commercially sensitive company information etc

* See SE's Data Protection Policy for definition of special category data.

There is no need to label Public or Internal information.

SE strongly recommends labelling correspondence, documents, and records which fall into the classification of "confidential" with a "Confidential" Header. This is however, at the discretion of the information owner/author based on the information's sensitivity and on how the information is intended to be handled and shared. Agreement to reclassify documents should be sought from the relevant business owner/team.

It is recommended that all personal data (eg HR information) is labelled as Confidential. However, there may be occasions when information (eg legal correspondence) is always handled as confidential but the

Confidential label may not be practical and is not always required. Information Asset Owners and team leaders should consider and agree what labelling is appropriate for their information.

Where Information Asset Owners and team leaders decide that labelling is not used for confidential information, the information must still be handled/processed as confidential and this must be communicated to their team and those who have access to their information.

If information is deemed to be Confidential or Confidential Sensitive and if labelling is required, labels should be applied as follows:-

Document

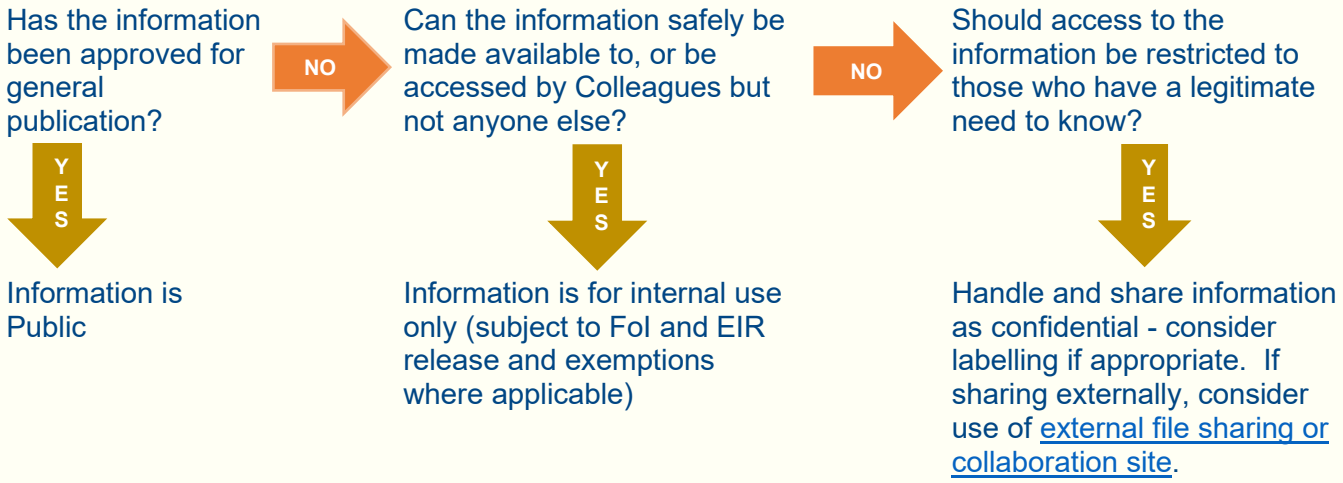
- At the top of the front/title page: '**Confidential' (**plus **Optional Information Identifier** - please **SEE** below).
- Within a document: 'Confidential' should be clearly marked at the top of every page within the document.
- Save your document on your team's SharePoint folders.

Email

- 'Confidential' should be included in the subject line of the email or Use Outlook Message Options to set Sensitivity level to: Confidential. (From your email message, select **File > Info > Properties.** Under Settings, select **Sensitivity** and then select **Confidential** from the drop-down list. Select **Close**.)
- All attachments deemed to be confidential should be marked as above.
- **NB** **SEE** essential requirement for encryption of attachments if recipient does not have a SE email address later in this document (*P9*).

NB Labelling information as Confidential does not necessarily exempt the information being provided in responses to FoI requests. Any information requested will be subject to an assessment under the FoI.

Deciding on which Information Classification is appropriate



For example:-

Public	Internal	Confidential
• Brochures • SE Annual Reports • Information published on SE's Websites • Advertising Materials	• Routine internal business email • Routine work in progress • Training materials • Meeting agendas • Information published on the Intranet	• HR Information • Personal Data (as defined by the (Data Protection legislation) • Negotiating positions • Pre-release publications • Draft Board Papers • Commercially confidential information relating to companies, suppliers or potential suppliers • Information subject to patent application

Note: Over time, some information will need to be reviewed and re-classified. For example, pre-release publications will move from Confidential to Public upon publication. Agreement to reclassify documents should be sought from the relevant Business Owner/Team.

Colleagues should also consider legal implications of information accessed or shared, eg whether it is subject to third party intellectual property rights such as copyright.

Optional Information Identifier

This may be used with 'Confidential' to indicate the users/groups that have a need to know that information.

For example:-

Information Asset	Optional Information Identifier
HR Information	CONFIDENTIAL - SENSITIVE
Sensitive Partner Information	CONFIDENTIAL - SENSITIVE (Group/Partner Name) Only
Very Limited distribution - Named individuals	CONFIDENTIAL - A Smith & B Jones ONLY

5. HOW TO HANDLE and SHARE INFORMATION

Prior to sharing information, consider –

WHAT information (Public, Internal or Confidential) am I storing/accessing/sharing?
WHERE is the information stored – an SE platform, site or system or a third party external platform, site or system?
WHO am I sharing the information with and/or from whom am I accessing/downloading this information?
HOW am I sharing and/or accessing this information?

The following scenarios provide advice based on these considerations

5.(a) STORING AND USING INFORMATION IN SE OFFICES OR WORKING AT HOME

Always lock your screen when you are away from your desk, even if it is only for a short period of time. If lost or stolen, report as soon as possible, following the Lost It, Report It procedure - **SEE** Loss of Information *(P12)*

I want to store electronic information on SE's systems	I want to store, copy, print or work on hardcopy in the office or at home	I want to dispose of hardcopy
Internal Information Store on your team's SharePoint folders, appropriate SE system or intranet. Regularly review and destroy records which are no longer required - **SEE** SE Retention Policy Personal development plans or early draft personal research may be stored on One Drive.	**Internal Information** Protect against accidental compromise to third parties at home and in the office. Apply a clear desk approach in all locations. In the office you should clear away at the end of the day in line with SE's Clear Desk Requirements. At home, maintaining a clear desk at the end of the day will reduce risk of accidental compromise to third parties.	**Internal Information** Check to confirm that the information does not require to be retained - **SEE** SE Retention Policy Must be disposed of only in the SE office recyclable paper waste bins or shredded in the office or at home.
Confidential Information Store on your team's SharePoint folders or appropriate SE system - ensure that file/folder permissions are set so that only those who 'need to know' have access. **SEE** SharePoint Online guidance.	**Confidential Information** Secure documents in a locked drawer, filing system or private space (area/drawer/cupboard not visible by others inside or outside your home) when away from your desk, office or home. Do not leave documents lying openly accessible in public areas. Ensure all documents are picked up promptly from the printer/copier. In the office, ensure 'secure print' is selected from the print menu. Avoid printing confidential documents at home if possible.	**Confidential Information** Check to confirm that the information does not require to be retained - **SEE** SE Retention Policy Must be disposed of by shredding in SE office or via SE office confidential waste bins. SE office shredders comply with auditable standards for shredding confidential information.

5.(b) CARRYING INFORMATION OUTSIDE SE OFFICES OR MY HOME

If lost or stolen, report as soon as possible, following the Lost It, Report It procedure - **SEE** Loss of Information (P12)

I want to carry electronic information outside an SE office or my home	**I want to carry hardcopy outside an SE office or my home (Note: The preferred method of carrying information outside SE is in electronic form on an SE approved encrypted device such as SE laptop, iPad, etc - SEE below)**
Internal Information Only use SE approved encrypted device in accordance with Using Scottish Enterprise IT Systems and Equipment. Do not let unauthorised people use your device. When using in a public place, use a privacy screen if practical and be aware of being overlooked. **SEE** Using Scottish Enterprise IT Systems and Equipment.	**Internal Information** Handle with due diligence. Protect against accidental compromise to third parties - carry in a closed folder or closed bag.
Confidential Information Try to avoid having Confidential documents on portable devices (including SE laptops, equipment hard drives). Avoid USB devices such as memory sticks as they are easily lost. If unavoidable follow the SE Internal handling requirements in accordance with Using Scottish Enterprise IT Systems and Equipment above *plus*: Ensure the information is encrypted and only on the device for the minimum time necessary. Obtain permission from the owner of the data.	**Confidential Information** There needs to be a clearly defined and unavoidable requirement to take confidential hard copy out with the office/home workspace. Should it be necessary, it needs to be secured, eg in a sealed, unclassified envelope, locked in a briefcase or hotel safe and take all practical steps to ensure it is secure. Never leave unattended if unsecured. If you require further advice contact our DPIGO or Records Management Team.

5.(c) SHARING INFORMATION WITH SE COLLEAGUES

If lost or stolen, report as soon as possible, following the Lost It, Report It procedure - **SEE** Loss of Information (P12)

I want to share or send electronic information to an SE Colleague. Where possible, share links to documents with SE Colleagues instead of attaching uncontrolled copies.	**I want to share or send hardcopy information to an SE Colleague**
Internal Information Use the SE email system and/or link to information on the intranet or to documents in SharePoint folders. As well as ensuring the most up to date version is accessed, the inclusion of links instead of attachments reduces carbon emissions.	**Internal Information** Sending hardcopy information should be avoided in so far as is possible. However, if it is not possible to share or send information in soft copy form (eg SE email, link to intranet or SharePoint folder), hardcopy must only be sent using 2nd class mail (**SEE** Post and Couriers Guidance).
Confidential Information **Verify recipients prior to sending by email.** 'Confidential' should be included in the subject line of the email or Use Outlook Message Options to set Sensitivity level to: Confidential. (From your email message, select **File > Info > Properties.** Under Settings, select **Sensitivity** and then select **Confidential** from the drop-down list. Select **Close**). Check the folder permission - restricted to the 'need to know' individuals. Do not use MS Teams Chat to share personal, sensitive or confidential information.	**Confidential Information** If the sharing of hardcopy documentation is specified in a contractual agreement, the agreed process should be followed. If no contractual agreement exists, sending hardcopy information should be avoided in so far as is possible. However, if it is not possible to share or send information in soft copy form (eg SE email, link to intranet or SharePoint folder), obtain permission from the owner of the information prior to copying and/or distributing to others. Use mail system - send in sealed envelope - consider using special delivery service. (**SEE** Post and Couriers Guidance).

5.(d) SHARING INFORMATION WITH and ACCESSING INFORMATION FROM THIRD PARTIES – 1 OF 5
Sending Information Only

If lost or stolen, report as soon as possible, following the Lost It, Report It procedure - **SEE** Loss of Information (P12)

I want to send electronic information to someone outside SE (eg Responses to Enquiries, Freedom of Information (FoI) or Subject Access requests (SAR)	I want to send hardcopy information to someone outside SE (eg Responses to Enquiries, Freedom of Information (FoI) or Subject Access requests (SAR)
Internal Information Email to external recipient only where there is an approved business need or other justification (eg Responses to enquiries, FoI, SAR request). **Verify the email address** of the recipient(s) and ensure they are aware that the information must only be used for the declared purpose. Avoid using USB devices. If unavoidable, only use SE approved, encrypted security checked devices approved by EIS in accordance with Using Scottish Enterprise IT Systems and Equipment.	**Internal Information** Send to external recipient only where there is an approved business need or other justification. **Verify recipient's address** prior to sending. External mail should be sealed - consider using special delivery service. (**SEE** Post and Couriers Guidance).
Confidential Information **Verify the email address of the recipient(s) prior to sending the email.** 'Confidential' should be included in the subject line of the email or Use Outlook Message Options to set Sensitivity level to: Confidential. Use the 7 Zip tool to create a compressed file attachment encrypted to the AES 256 standard. Set a strong, complex encryption password. Communicate password verbally or in separate email after confirming receipt of encrypted files. Do not reuse a previous password. **SEE** advice on setting strong passwords. Send to external recipient only on a 'need to know' basis where there is an approved business, contractual or legislative need (eg FoI, SAR) and advise the originator/information owner. Ensure that the external recipient knows the classification level and is aware of the protection requirements.	**Confidential Information** Share with someone outside SE only on a 'need to know' basis when electronic transmission is not possible, where there is an approved business, contractual or legislative need and advise the information owner. No security marking should appear on the outer envelope. Double envelopes are required. Courier/special mail is the recommended option. (**SEE** Post and Couriers Guidance).

5.(e) SHARING INFORMATION WITH THIRD PARTIES - 2 OF 5
SE Secure External File Sharing or Collaboration Site - FileShare Scotland or MS Teams Team

If lost or stolen, report as soon as possible, following the Lost It, Report It procedure - **SEE** Loss of Information (P12)

I want to create/host a secure SE file sharing or collaboration platform via SE's organisational platforms/sites (eg FileShare Scotland or MS Teams) to share information with trusted partners or third parties.

Internal Information

Refer to the External File Sharing Site process to create a secure external file sharing site.

Do not post or share information outside the closed user group - **ensure group membership is appropriate for the 'need to know' and there is an approved business, contractual or legislative need.**

Where group members are required to gather or share information on a dynamic collaboration document, Colleagues may update the information required.

When using an MS Teams Team site for collaboration, information containing decisions and approvals can be shared via Posts within Channels - SEE MS Teams guidance for further details on Posts and Channels

Attention should be paid to the group membership and their 'need to know' the information being posted regardless of the information's format (ie document, image, conversation etc).

Confidential Information

Sharing confidential information on SE hosted file sharing or collaboration sites is permitted where there is an approved business, contractual or legislative need to share confidential information on a 'need to know' basis. Refer to the External File Sharing Site Process to create a secure file sharing site.

A Data Sharing Agreement may be required. SEEK advice from Legal Services or DPIGO.

If personal information is to be shared, a Data Protection Risk Assessment (DPIA) will be required.

When using an MS Teams Team site for collaboration, containing confidential information, decisions and approvals can be shared via Posts within Channels - SEE MS Teams guidance for further details on Posts and Channels

Attention should be paid to the group membership and their 'need to know' the information being posted regardless of the information's format (ie document, image, conversation etc).

5.(f) SHARING INFORMATION WITH AND ACCESSING INFORMATION FROM THIRD PARTIES - 3 OF 5
Security Risk Assessed Third Party Hosted External File Sharing or Collaboration Platforms

If lost or stolen, report as soon as possible, following the Lost It, Report It procedure - **SEE** Loss of Information (P12)

I want to access and/or share information on a SE/EIS security risk assessed file sharing platform hosted by a trusted third party (such as Government, public sector partner, industry body, client)

Internal Information

It is SE's preference that information shared either by and/or with SE, is accessed and controlled via SE's organisational platforms/sites (SEE - External File Sharing Site process.)

However, there are circumstances where Colleagues are invited to access or shared information via a site/platform created by a trusted third party. The most commonly used platforms/sites for file sharing/collaboration have been security risk assessed by SE and EIS as having appropriate technical controls in place. (SEE Third Party Hosted File Sharing Site process for list of risk assessed file sharing/collaboration platforms), Colleagues may access and download third party files and may share files and documents created by SE where required and in line with the classification labels set out above.

Where the third party hosted site is created for the purpose of gathering information from members on a dynamic collaboration document, Colleagues may update the information required.

Online conversations in these sites are permitted. At all times, Colleagues should be aware of what is being accessed and/or shared and with whom.

Attention should be paid to the group membership and their 'need to know' the information being posted regardless of the information's format (ie document, image, conversation etc).

Confidential Information

Downloading and viewing confidential information on a third party security risk assessed site is permitted - SEE External File Sharing Site Process. Sharing and uploading confidential information on file sharing and/or collaboration sites hosted by others should be avoided.

Where there is an approved business, contractual or legislative need to share confidential information on a 'need to know' basis, please refer to the External File Sharing Site process.

A Data Sharing Agreement may be required. SEEK advice from Legal Services or DPIGO.

If personal information is to be shared, a Data Protection Risk Assessment (DPIA) will be required.

Online conversations in these sites are permitted. At all times, Colleagues should be aware of what is being accessed and/or shared and with whom.

Attention should be paid to the group membership and their 'need to know' the information being posted irrespective of the information's format (ie document, image, conversation etc).

5.(g) SHARING INFORMATION WITH AND ACCESSING INFORMATION FROM THIRD PARTIES - 4 OF 5
Non-Security Risk Assessed Third Party Hosted External File Sharing or Collaboration Platform

If lost or stolen, report as soon as possible, following the Lost It, Report It procedure - **SEE** Loss of Information (P12)

I want to access and/or share information on a non-security risk assessed file sharing or collaboration platform hosted by a third party.

Internal Information

Sharing information on external file sharing or collaboration sites/platforms which have not been security risk assessed by SE and EIS should be avoided.

It is SE's preference that information shared by and with SE is accessed and controlled via organisational platforms/sites above (SEE - SE's External File Sharing Site process) or encourage third party to use a SE/EIS security risk assessed platform (SEE above).

(i) Access to non-security risk assessed sites/platforms for **sharing information and collaborating** purposes will require security assurances to be provided by the third party - SEE External File Sharing Site Process
If the site/platform is assessed as having satisfactory technical controls implemented to secure the site/platform, Colleagues may access and share files and documents created by SE where required and in line with the classification labels set out above.

If the site is approved, online conversations in these sites are permitted. Be aware of what you share and with whom.

Attention should be paid to the group membership and their 'need to know' the information being posted irrespective of the information's format (ie document, image, conversation etc).

(ii) Security risk assessments are not required for access to non-security risk assessed sites/platforms for the purpose of download/**read only or to complete online forms** within a brief limited period. SEE - External File Sharing Site process

Confidential Information

Sharing confidential information on file sharing or collaboration sites/platforms hosted by others, which have not been security risk assessed by SE and EIS should be avoided.

Where there is an approved business, contractual or legislative need to share confidential information on a 'need to know' basis, it is SE's preference that information shared by and with SE is accessed and controlled via SE's organisational platforms/sites (SEE 5e above).

If this is not practical, encourage the third party to use a SE/EIS security risk assessed platform (SEE 5.(f) above).

(i) Access to non-security risk assessed sites/platforms for sharing confidential information and collaborating purposes will require security assurances to be provided by the third party* - SEE External File Sharing Site Process

If the site/platform is assessed as having satisfactory technical controls implemented to secure the site/platform, Colleagues may access and share confidential information, including information created by SE where required and in line with the classification labels set out above.

If the site is approved, online conversations in these sites are permitted. Be aware of what you share and with whom.

Attention should be paid to the group membership and their 'need to know' the information being posted irrespective of the information's format (ie document, image, conversation etc).

(ii) Security risk assessments are not required for access to non-security risk assessed sites/platforms for the purpose of **downloading/read only confidential information** within a brief limited period. SEE - External File Sharing Site process.

5.(h) SHARING INFORMATION WITH THIRD PARTIES - 5 OF 5
Social Networking Sites, Verbal or Online Discussions

If lost or stolen, report as soon as possible, following the Lost It, Report It procedure - **SEE** Loss of Information (P12)

I want to share information on a social networking site	I want to discuss with someone (face to face/phone call/ MS Teams or other online call/ MS Teams Chat/other online "chat")
Internal Information Do not post information outside a closed user group - ensure group membership is appropriate for the 'need to know'. Please **SEE** the SE Social Media Policy.	**Internal Information** Use discretion. Ensure the conversation cannot be overheard by non-SE personnel. You should also disable any listening devices, eg Alexa, Google Assist, Siri etc if they are within earshot when you are on a call. Chat between individuals or groups in MS Teams or other online chat and meeting platforms should only be used for informal discussion and not for sharing confidential information, approvals etc. Chat can be viewed by all those invited to attend the meeting (including guests and non-attendees). Do not use MS Teams or other online meeting Chat for approvals or more formal communications. MS Teams Chat is subject to FoI and Data Protection legislation - be aware of what you share. **SEE** Using Chat.
Confidential Information Not allowed.	**Confidential Information** Ensure the conversation cannot be overheard by those with no 'need to know'. Do not leave confidential information on voicemail systems. Disable any listening devices, eg Alexa, Google Assist, Siri etc if they are within earshot when you are on a confidential call. Do not use MS Teams Chat to share personal, sensitive or confidential information. **SEE** Using Chat.

5.(i) LOSS OR UNINTENDED SHARING OF INFORMATION		
What has happened to the information?	**What is the impact?**	**What are the rules?**
I have lost my laptop, mobile phone, removable media (eg USB/memory stick; cd) or work documents. I have accidentally shared confidential information with an unintended audience via email, public place etc.	May lead to a Breach of Contract or Data Breach where sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorised fashion.	Report as soon as possible, following the Lost It, Report It procedure.

6. NON-SE CLASSIFICATIONS

Partner organisations may share information with SE that is marked with their classification. This information must be handled in accordance with the contractual arrangement with the information owner. If the information owner has not defined any handling rules you should handle the information as if it had an SE classification.

The table below maps Government, Corporate and SE classification.

Government Protective marking	Common Business terms	SE Classification
Top Secret		Not held by SE
Secret	Confidential	CONFIDENTIAL
Official-Sensitive	Confidential	CONFIDENTIAL
Official	For internal use only	INTERNAL
Official	Publicly Available	PUBLIC

7. RELATED LEGISLATION, POLICIES AND DOCUMENTS

- SE Retention Policy
- SE Data Protection Policy
- Using Scottish Enterprise IT Systems and Equipment
- SE Social Media Policy
- SE Code of Conduct
- SE Information Security Policy
- Data Protection Act 2018
- Environmental Information (Scotland) Regulations 2004,
- Freedom of Information (Scotland) Act 2002
- INSPIRE (Scotland) Regulations 2009
- Public Records Scotland Act 2011
- Re-use of Public Sector Information Regulations 2015.

8. PERSONAL DATA AND PRIVACY STATEMENT

Whenever personal data is processed under activities regulated by this Policy, such processing will be done in accordance with our Data Protection Policy and our External Privacy Notice for third parties and Internal Privacy Notice for Colleagues.

9. DOCUMENT REVISION HISTORY

Review of policy

This policy will be reviewed as a minimum every 2 years or at times of significant legislative or organisational changes.

Revision History

Version	Date	Author	Description of changes	Status	Approved by
1.0	Oct 2010	Chris Knight (EIS) Mandy Bell	• Final Version 1	Approved	Business Security Forum
2.0	Jun 2014	Chris Knight (EIS) Mandy Bell	• Added Confidential Sensitive category • Amended 'Mandatory labelling' policy to 'non-mandatory, at discretion of author'	Approved	Business Security Forum
3.0	Mar 2021	Mandy Bell	• Included ref to Lost It, Report It procedure • Included scenarios for sharing information via secure and publicly available file sharing and collaboration sites • Updated to include home working scenarios • Relevant supporting legislation added to policy • Policy template used to make format changes	Approved	Head of Governance and Office Services
4.0	Oct 2021	Mandy Bell	• Introduction reworded • Advice on using SE hosted external file sharing and collaboration sites updated. • Advice on using third party hosted external collaboration sites updated. • Advice denying the use of Dropbox removed.	Approved	Senior Information Risk Owner