SCOTTISH QUALIFICATIONS AUTHORITY

POLICY NAME	Information Security
VERSION NUMBER	5.0
POLICY AUTHOR	Jocelyn Martin
POLICY OWNER	Maidie Cahill
BUSINESS AREA OWNER	Strategic Planning & Governance
POLICY EFFECTIVE FROM	9 January 2017
POLICY REVIEW DATE	9 January 2018
NEW/REVISED POLICY	Revised

What does this policy apply to?	This policy applies to all of SQA's information and information systems. It applies to any systems attached to SQA's computer or telephone networks. It applies to all information processed by SQA in both electronic and hard copy, and any communications sent to or from SQA.
Who does the policy apply to?	This policy applies to all users of SQA's information and information systems (employees, agency workers, consultants, and others with authorised access to SQA's information or systems) This policy also applies to suppliers that provide services to SQA in respect of information processing facilities and business activities.
What support is available to help SQA implement this policy?	Contact a member of the Information Governance team by phone, or e-mail at information.governance@sqa.org.uk.

1. Introduction

This policy forms part of a suite of policies to support the effective and safe use of SQA's information and information systems.

Information security must be an integral part of information management, whether the information is held electronically or in hard copy. SQA is committed to protecting the security of its information and information systems in order to ensure that

- the integrity of SQA's information is maintained, so that it is accurate and fit for purpose.
- information is available to those who need it and there is no disruption to SQA's business.
- confidentiality is not breached, and SQA's information is accessed only by those authorised to do so.
- SQA complies with its legal obligations, including those applicable to personal data under the Data Protection Act 1998 (DPA).

2. Purpose

This policy provides a framework for the management of information security across SQA.

3. Scope

This policy applies to all users of SQA's information and information systems.

4. Responsibilities

Information security is the responsibility of everyone who works for, or on behalf of, SQA. All users have a role to play in putting the necessary controls in place, and complying with these controls to keep SQA's information secure. Some individuals/grades have specific responsibilities, as detailed below.

Executive Management Team	• Approves Information Security Policy and related information policies • Promotes adoption and compliance
Director of Corporate Services & SIRO (Senior Information Risk Owner)	• Owner of Information Security Policy and related information policies • Member of the Information Governance Steering Group(IGSG)
Heads of Service	• Ensure that staff, and where necessary other individuals engaged by SQA, undertake mandatory training, and ongoing training needs are routinely assessed • Have responsibility for the management of data within their respective business areas • Have responsibility for creating business continuity plans to ensure that any interruption can be recovered • Ensure that only authorised staff have access

	to systems in their business area • Report performance of the Information Security Management System (ISMS) for 27001 (applicable teams only)
All users	• Comply with this and other information policies and related procedures • Report any security incident or 'near miss' in accordance with the Security Incident Management procedures • Undertake information security training as required by SQA
Information Governance Manager	• Provides advice and support on information legislation and compliance with ISO 27001 • Develops and provides suitable training for all staff • Co-ordinates, manages and advises on responses to security incidents • Reports performance of the ISMS for ISO 27001
IT Security Manager	• Provides technical advice on matters relating to IT security and ensures compliance of IT systems • Implements effective security measures to reduce the level of threat to IT systems • Reports performance of the ISMS for ISO 27001
Facilities Manager	• Responsible for physical security of all SQA sites • Reports performance of the ISMS for ISO 27001
Third Parties and Contractors	• Comply with confidentiality / information security agreements (where potential or actual access to information is identified)
Information Governance Steering Group	• Strategic oversight of information security • Oversight of ISO 27001 certification

5. Personal Information

5.1 *Data Protection Act*

Personal data must be handled in accordance with the Data Protection Act 1998 (DPA) and in accordance with SQA's Data Protection Policy and related guidance. The DPA requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data.

A higher level of security should be provided for 'sensitive personal data', which is defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences.

5.2 *SQA's personal data*

SQA holds personal information about candidates, employees, centre staff, appointees and others. Line managers must provide staff with clear guidance on what personal information may be stored and the circumstances under which personal information may be released.

SQA has a duty of care in the way it uses personal information and in to whom it is disclosed. Since there are laws governing the use of personal information, individuals and SQA could be prosecuted for failing to comply with the legal requirements.

6. **Protecting our Information**

SQA has a range of controls in place to ensure that personal and business-sensitive information is protected.

6.1 Security education and training

All new employees are required to read and accept the Information Security Policy and to complete the Protecting Information online training course within 28 days of joining SQA. All employees must complete the online training course on any subsequent occasions as required by the Information Governance team.

All employees and other users of SQA's information and information systems must comply with any request to complete training related to the protection of SQA's information.

6.2 *Access controls*

6.2.1 Physical security

Photo ID Proximity Cards
Staff and other authorised users are provided with photo ID badges by Facilities Management. ID badges must be worn at all times whilst on SQA premises. Visitors are provided with visitor badges. Facilities staff will carry out random security checks to ensure that badges are being worn.

Users must not permit access to the building or floor to anyone who is not in possession of an SQA ID card or visitor badge. Anyone without a badge must be escorted to reception.

If an SQA ID card or visitor badge is lost, it must be reported immediately to reception.

Building access
Staff and other authorised users will be given access to any areas of SQA premises which are not restricted. Access to restricted areas will be strictly controlled.

Visitors must register at reception on arrival and be escorted **at all times**.

CCTV
CCTV is deployed at SQA’s premises to provide added security. CCTV systems are in operation on both sites for the purposes of staff safety and the prevention of crime.

See the CCTV Policy for detailed information about the use of CCTV.

6.2.2 Access to IT systems

All new users are required to read the IT and Information Security form before gaining access to SQA’s IT systems. This form will be issued to new employees via the meta-compliance process and users will be required to accept the conditions for access. Agency workers may be required to sign a hard copy version of the form.

- Permanent employees will be given ongoing access, which will be removed once an employee leaves SQA’s employment.
- Agency workers or employees on fixed-term contracts will be given access for the duration of their contract.
- Other users will be given access for a limited time, dependent on the reason for their access.

Users will be granted access in line with the IT Access Control Policy.

Requests for additional access must be made by raising a ticket with the IT Service Desk. Access must only be requested to systems which the user requires for the performance of their duties. The user is responsible for arranging for access to be removed when it is no longer necessary for the performance of their duties.

6.2.3 User access controlled within teams

Where user access to an IT system is controlled within a business area it is the responsibility of the individual(s) managing that access to ensure that they comply with the IT Access Control Policy. This means ensuring that: access permissions are relevant to a user’s role; access is adjusted or removed when the user changes their role or leaves SQA; and that reviews of access rights are undertaken on a regular basis.

See the IT Access Control Policy for information.

6.2.4 Access to SQA premises and IT systems outwith normal hours

Members of staff who require access to SQA premises and IT systems outwith normal working hours must request out-of-hours access.

See the Security Procedures on the Policy & Guidelines register for information on how to request access.

6.2.5 Passwords

Passwords are an important aspect of information security and must be protected. The use of strong passwords helps to prevent unauthorised access to systems, but users also need to keep these passwords secure.

Do not

- share a password with anyone at SQA, including IT staff and line managers
- share a password with anyone outside of work
- insert a password into an e-mail message
- log someone else into an SQA IT system
- reveal a password over the telephone, to anyone
- reveal a password on security forms or questionnaires
- use the same password for other accounts
- use predictable passwords containing personal information such as names, username or date of birth

If a user suspects that their password has been compromised they must contact the IT Service Desk immediately and report it as a security incident, using the Security Incident Report form.

6.3 IT equipment

SQA permits access to SQA systems and information **only** on SQA-provided equipment, which is encrypted. This applies to all IT equipment and portable devices, ie desktops, laptops, tablets, smart phones and memory sticks.

Users must not routinely save any personal or business-sensitive information to a portable device. Users must store information on the appropriate corporate system on the network to ensure version control.

6.3.1 Memory sticks

Memory sticks must only be used for a temporary and specific purpose and must not be used to store information.

6.3.2 CDs and DVDs

CDs and DVDs are not backed-up and are liable to degrade, therefore they should not be used to store information unless there is clear justification for their use. If this is the case, contact a member of the Information Governance team to discuss the requirement.

6.3.3 Overseas travellers on SQA business

Certain countries place restrictions on the use of encrypted laptops and other portable devices. Before travelling internationally on SQA business, users must ensure that they have obtained the most up-to-date information about travelling with encrypted equipment, and act accordingly.

Where there is **any** potential risk to the individual travelling with encrypted equipment, travellers must take unencrypted equipment. In these circumstances travellers **must not** save or transfer personal information onto unencrypted equipment, and must take extra care of equipment which contains any business-sensitive information.

See the International Travel Policy for detailed information about travelling overseas with IT equipment.

6.4 E-mail security

Users must bear in mind that e-mail is not a confidential means of communication. Before sending an email, apply the following “bulletin board” test:

- Would you be happy to post the contents of your e-mail as a bulletin for all to see?

There are many ways in which e-mail messages can be read by those for whom they were not intended. E-mails can be:

- wrongly addressed
- forwarded accidentally
- intercepted by third parties (legally or otherwise)
- forwarded by initial recipients to third parties against the wishes of the sender
- viewed accidentally on recipients’ screens

See the E-mail Policy for more detailed information about the use of e-mail.

6.5 Instant messaging

Instant messaging (IM) enables a user to communicate with another user in real time using text. Users must note that

- personal information must not be sent via IM under any circumstances.
- IM must not be used for any information which should, or has the potential to, be retained as a record.

6.6 Remote and home-working

SQA supports staff who travel for work, are home-based, or who occasionally work at home, by enabling staff to connect to the SQA network remotely using a Virtual Private Network (VPN). The use of a VPN supports the safe use of electronic information.

Users should be aware of their environment

- Users must ensure that information is not left unattended on screens, for family members or other individuals to read. Screens must be locked when not in use.

6.7 Travelling on public transport

Users should be aware of their environment

- Sensitive/confidential phone calls should be avoided or conducted where they cannot be overheard.
- Portable equipment must be kept close-by and not left unattended.

- Business-sensitive information should not be viewed whilst travelling, unless the user is confident that they are not overlooked.

6.8 Electronic documents

Before publishing a document on SQA's website users should remove personal information, such as author and contributor names, from the document being published, as these details can be used for social engineering[1] attacks.

See the Appendix for information on how to do this.

6.9 Hard copies

6.9.1 Storage

Wherever practicable, documents containing personal or business-sensitive information should be stored in locked cupboards, drawers or cabinets. Where this is not practicable, and information is kept on open shelving, the room must be locked when unoccupied.

Keys to cupboards, drawers or cabinets should not be left on open display when the room is unoccupied.

6.9.2 Removal from SQA premises

Personal or business-sensitive information must only be taken off-site if the reason is specifically related to a job role, or remote or home-based working, or where permission has been obtained from a user's line manager. Where this is necessary, or prior approval has been obtained, extra care must be taken to keep this information secure whilst in transit and off site.

Where it is necessary to use personal or business-sensitive information at home, users must return the information to SQA premises, or arrange for it to be destroyed securely, as soon as possible after the user no longer requires the information. Users must also ensure that personal or business-sensitive information used at home complies with retention requirements as set out in the relevant retention schedule.

Users should not normally read on public transport any papers containing personal or business-sensitive information. This is permitted only if the user is satisfied that the content can in no way be read by people adjacent to, or near to them.

6.9.3 Transmission

Internal mail - Confidential documents should, where possible, be hand-delivered. If they can't be hand-delivered they should be placed in a sealed envelope marked 'To be opened by addressee only'.

[1] Social engineering in this context involves tricking individuals into divulging confidential information by masquerading as a member of staff

External mail – Confidential documents should be sent using an SQA-approved courier or special delivery option. This does not apply to documents sent for recruitment purposes, which can be sent via first class post. The sender must ensure that the envelope is properly secured and correctly addressed.

Fax – If confidential documents are to be faxed, the sender must ensure they use the correct fax number and that the recipient is near to, or waiting at, the receiving fax, to collect the information when it arrives.

6.9.4 Disposal

Documents containing personal, sensitive personal or business-sensitive information must be disposed of in a confidential manner, either by shredding or by placing in confidential waste bags.

7. Suppliers and Third Parties

SQA must ensure that the suppliers it engages act responsibly and protect SQA’s personal and business-sensitive information. To ensure this happens the following actions must be taken.

- Tender documents must detail the security requirements necessary to mitigate the risks associated with access to SQA’s information.

- Agreements with third parties involving accessing, processing, communicating or managing SQA’s information, or information systems on behalf of SQA, should cover all relevant security requirements, and be covered in contractual arrangements.

- All suppliers and third parties who require access to networks, computer systems or personal information, must comply with this policy.

- Failure by a supplier to meet SQA’s minimum security requirements should preclude that supplier from continuing with the tender process, unless there are justifiable reasons for allowing them to continue.

- Contracts should be subjected to regular review, which includes an assessment of information security compliance.

All new suppliers must undergo evaluation of their information security arrangements to ensure that they have implemented sufficient controls to support SQA’s requirements. A checklist is available from the Procurement team to support the evaluation process.

8. Security Incidents

A security incident can be defined as any actual or potential event which has, or may have, compromised the confidentiality, integrity or availability of SQA’s information.

The impact of a security incident relating to SQA’s information may be on

- confidentiality - disclosure of confidential information to an unauthorised person
- integrity – the accuracy or completeness of information is put at risk
- availability – information or an information system may not be available

A security incident might occur due to accidental or deliberate destruction, loss, alteration, or disclosure, of SQA's information. A security incident could be caused in a number of ways, such as

- loss/theft
- insufficient access controls
- equipment failure
- human error
- hacking attack
- deception
- security weakness

A security weakness is a vulnerability which can be exploited resulting in a security incident. It is typically identified from existing systems or practices, rather than being a sudden event.

All security incidents, including weaknesses, must be reported.

*See the **Security Incident Management Procedures** for details about reporting an incident, or contact a member of the Information Governance team for advice.*

9. Return/Disposal of IT Equipment

SQA IT equipment must be returned to Business Systems in the following circumstances:

- When the reason for being supplied with SQA equipment has ended, eg on leaving SQA's employment or at the end of a contract

- When the SQA equipment is no longer required by the person to whom it was allocated (IT equipment must not be re-allocated within a team without the permission of Business Systems)

All IT equipment, including portable devices such as memory sticks, must be disposed of securely by Business Systems staff. Returned equipment will be re-allocated or securely destroyed.

10. Compliance

10.1 Disciplinary action

It is extremely important that all users read and understand this policy, and comply with it. Non-compliance with this policy may constitute a disciplinary offence which may result in disciplinary action being taken against the user.

If a user thinks that they may have breached this policy, they should speak to their line manager or Head of Service as soon as possible. The line manager or Head of Service should then contact HR or the Information Governance team for advice. Failure to report a breach timeously may constitute a further disciplinary offence.

10.2 Continual improvement

SQA is committed to improving information security, and will do this by

- seeking opportunities for improvement through holding regular meetings of the Information Governance Steering Group (IGSG).

- identifying appropriate organisation-wide security measures. These measures will be evaluated by the IGSG, and where actions are identified to improve information security, they will be implemented.

- producing an annual report on information security in SQA, for discussion at Audit Committee.

10.3 Interested parties

This policy will be made available to certain external interested parties who have a specific requirement to comply with, or be aware of, SQA's Information Security Policy (as specified in tender/bid documents or contracts).

11. SQA Policies and Legislation

This policy should be read in conjunction with the following SQA policies which are reviewed and updated as necessary to meet SQA's business needs and legal obligations.

- IT Acceptable Use Policy
- Data Protection Policy
- E-mail Policy
- Clear Desk and Clear Screen Policy
- IT Access Control Policy
- International Travel Policy
- Freedom of Information (Scotland) Policy
- Records Management Policy
- Retention and Disposal Policy
- Anti-bribery and Corruption Policy
- CCTV Policy
- Home Based Worker Policy
- Flexible Working Policy
- Copyright Policy
- Dispute Resolution Policy

The following documents are also relevant.

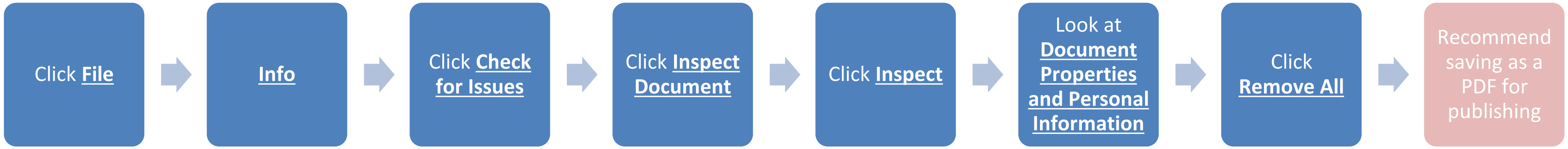
- Security Incident Management Procedures
- Security Procedures
- Dispute Resolution Procedures

This policy respects and complies with the following applicable laws.

- Data Protection Act 1998
- Freedom of Information (Scotland) Act 2002
- Regulation of Investigatory Powers (Scotland) Act 2000 (RIPA)
- Privacy in Electronic Communications Regulations 2003
- Human Rights Act 1998
- Computer Misuse Act 1990
- Equality Act 2010
- Civic Government (Scotland) Act 1982
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Protection of Children Act 1978
- Protection from Harassment Act 1997
- Defamation Act 2013
- UK Bribery Act 2010
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

How to remove personal information from documents to be published

When a Microsoft word document* is **open**


Click **File**

Info

Click **Check for Issues**

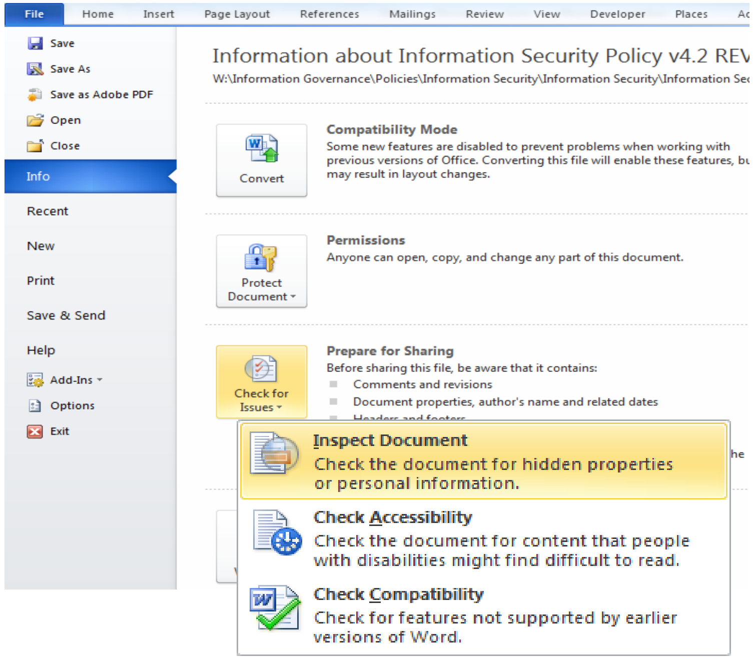
Click **Inspect Document**

Click **Inspect**

Look at **Document Properties and Personal Information**

Click **Remove All**

Recommend saving as a PDF for publishing



Information about Information Security Policy v4.2 REV

W:\Information Governance\Policies\Information Security\Information Security\Information Sec

Compatibility Mode
Some new features are disabled to prevent problems when working with previous versions of Office. Converting this file will enable these features, bu may result in layout changes.

Permissions
Anyone can open, copy, and change any part of this document.

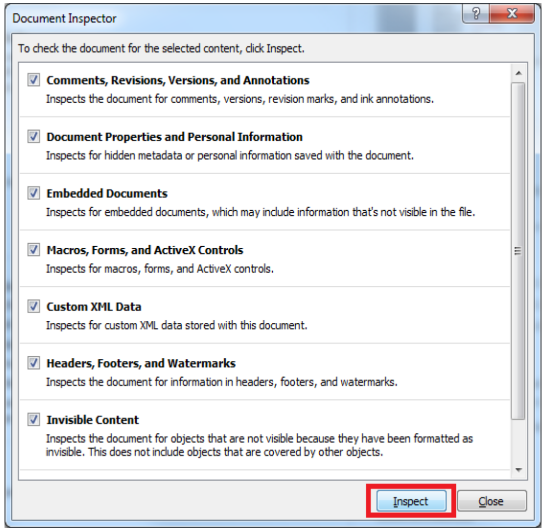
Prepare for Sharing
Before sharing this file, be aware that it contains:

- Comments and revisions
- Document properties, author's name and related dates
- Headers and footers

Inspect Document
Check the document for hidden properties or personal information.

Check Accessibility
Check the document for content that people with disabilities might find difficult to read.

Check Compatibility
Check for features not supported by earlier versions of Word.


Document Inspector

To check the document for the selected content, click Inspect.

☑ **Comments, Revisions, Versions, and Annotations**
Inspects the document for comments, versions, revision marks, and ink annotations.

☑ **Document Properties and Personal Information**
Inspects for hidden metadata or personal information saved with the document.

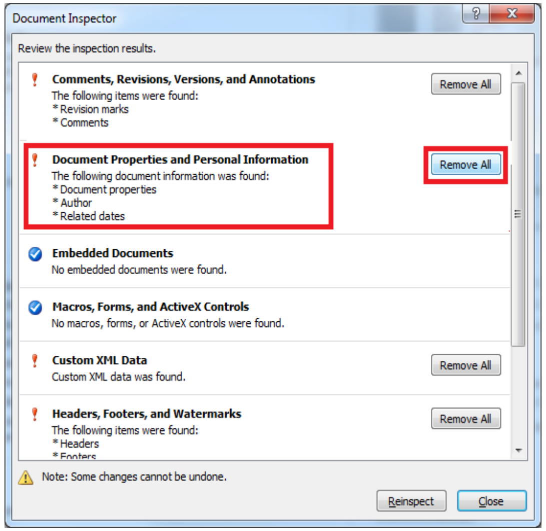
☑ **Embedded Documents**
Inspects for embedded documents, which may include information that's not visible in the file.

☑ **Macros, Forms, and ActiveX Controls**
Inspects for macros, forms, and ActiveX controls.

☑ **Custom XML Data**
Inspects for custom XML data stored with this document.

☑ **Headers, Footers, and Watermarks**
Inspects the document for information in headers, footers, and watermarks.

☑ **Invisible Content**
Inspects the document for objects that are not visible because they have been formatted as invisible. This does not include objects that are covered by other objects.


Document Inspector

Review the inspection results.

Comments, Revisions, Versions, and Annotations
The following items were found:
* Revision marks
* Comments

Document Properties and Personal Information
The following document information was found:
* Document properties
* Author
* Related dates

Embedded Documents
No embedded documents were found.

Macros, Forms, and ActiveX Controls
No macros, forms, or ActiveX controls were found.

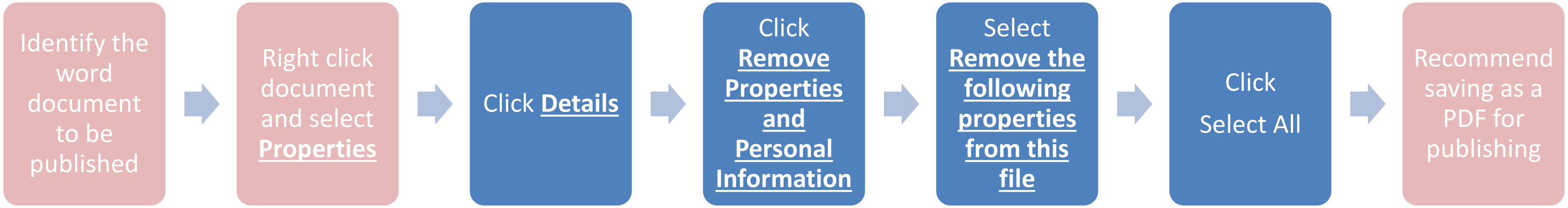
Custom XML Data
Custom XML data was found.

Headers, Footers, and Watermarks
The following items were found:
* Headers
* Footers

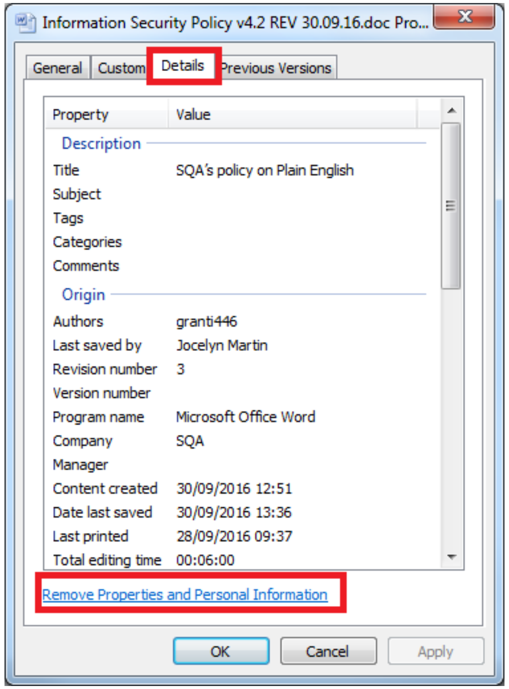
Note: Some changes cannot be undone.

**This is also applicable to other Microsoft products such as excel*

When a Microsoft word document* is **closed**



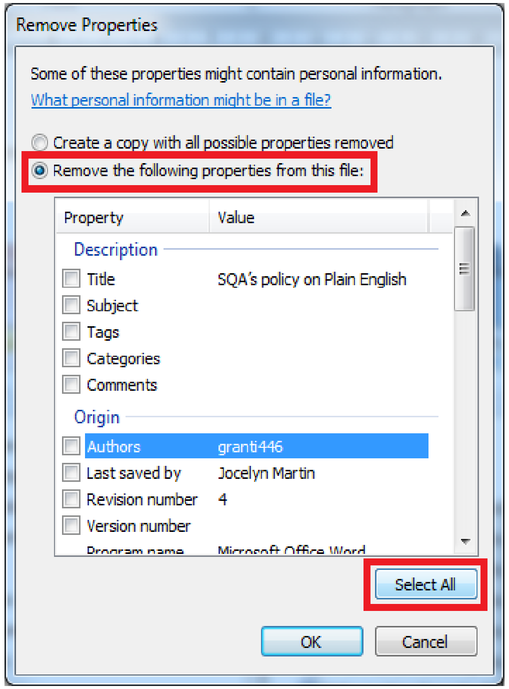
Identify the word document to be published → Right click document and select **Properties** → Click **Details** → Click **Remove Properties and Personal Information** → Select **Remove the following properties from this file** → Click Select All → Recommend saving as a PDF for publishing



Information Security Policy v4.2 REV 30.09.16.doc Pro...

Property	Value
Description	
Title	SQA's policy on Plain English
Subject	
Tags	
Categories	
Comments	
Origin	
Authors	granti446
Last saved by	Jocelyn Martin
Revision number	3
Version number	
Program name	Microsoft Office Word
Company	SQA
Manager	
Content created	30/09/2016 12:51
Date last saved	30/09/2016 13:36
Last printed	28/09/2016 09:37
Total editing time	00:06:00

Remove Properties and Personal Information



Remove Properties

Some of these properties might contain personal information.
What personal information might be in a file?

○ Create a copy with all possible properties removed
● Remove the following properties from this file:

Property	Value
Description	
□ Title	SQA's policy on Plain English
□ Subject	
□ Tags	
□ Categories	
□ Comments	
Origin	
□ Authors	granti446
□ Last saved by	Jocelyn Martin
□ Revision number	4
□ Version number	
Program name	Microsoft Office Word

**This is also applicable to other Microsoft products such as excel*