Tees, Esk and Wear Valleys
NHS Foundation Trust

Public – To be published on the Trust external website

Information Asset Register Procedure

Ref IT-0010-001-v2

Status: Approved
Document type: Procedure

Contents

1 Purpose

The purpose of this document is to provide guidance on:-

- Populating and maintaining information asset registers;
- Requesting a new asset register;
- Disposing of and archiving asset registers;
- Treating and managing risk via the Information Asset Risk Assessment form.

2 Related documents

This procedure describes what you need to do to safeguard Trust information assets in line with the Information Security and Risk Policy.

This procedure also refers to:-

- ✓ Introduction or Upgrade of Information Systems Policy

3 Information Risk Management Documents

All information risk management documents are held in the Information Risk Management folder on the Trust-wide shared drive.

Access is via T:\Information Risk Management and is open to all staff.

These documents include:-

- Information mappings;
- Information asset registers;
- Overarching information asset register;
- Trust-wide information asset register;
- Training needs assessments;
- Amendment forms;
- Monitoring and reporting;
- Briefings.

3.1 Information Mapping

- This is a process of documenting all flows of person-identifiable and business-sensitive information. Mapping shows us how information moves through the Trust, who we share it with, how it is protected in transit and the legal basis for processing and sharing. All flows are given a risk assessment that is determined by the level of protection given to the data whilst in transit.

- Information Mapping is done initially by the IAA with a member of Information Department's Compliance team, and maintained through regular review by the IAA, when ways of working change or new ways of working are introduced.
- The information mapping process focusses on any information flows that are unique to the team, or which are done differently in that team or locality compared to other areas.
- All information flows are recorded centrally and form the Trust's Record of Processing Activity.

3.2 Information Asset Registers

Information Asset Registers are created by Information Department's Compliance team and maintained by IAAs with IAAAs in consultation with their IAO. Asset registers show what information assets are held and used by the team for which the IAA is responsible.

Information assets are risk assessed at a Trust level within the Trust-wide information asset register (see below). The IAA will only risk assess information assets if the team works differently to the Trust standard, e.g. non-Trust premises, the team includes staff from other organisations, etc.

3.3 Overarching Information Asset Register

This is the Trust's audit trail of what IARs are currently in use, new ones that have been requested, plus old IARs that have been archived. It also holds the passwords to allow editing of the IARs. Access to the Overarching Information Asset Register is therefore restricted to INFORMATION DEPARTMENT only, although information held on it will be shared as appropriate.

3.4 Trust-wide Information Asset Register

The Trust-wide information asset register gives the risk ratings for information assets that are held and used to a set standard (i.e. Trust staff working in Trust premises). This means IAAs do not need to carry out risk assessments unless they and their team work differently

3.5 Training Needs Assessments

Training Needs Assessments are carried out by Information Department's Compliance Team with the IAA and their team to determine the team's understanding of information/data security and risk. Focussed training and support can be provided by Compliance Team where needed.

3.6 Amendment Forms

These are used to request a new IAR or archive an old IAR.

3.7 Monitoring and Reporting

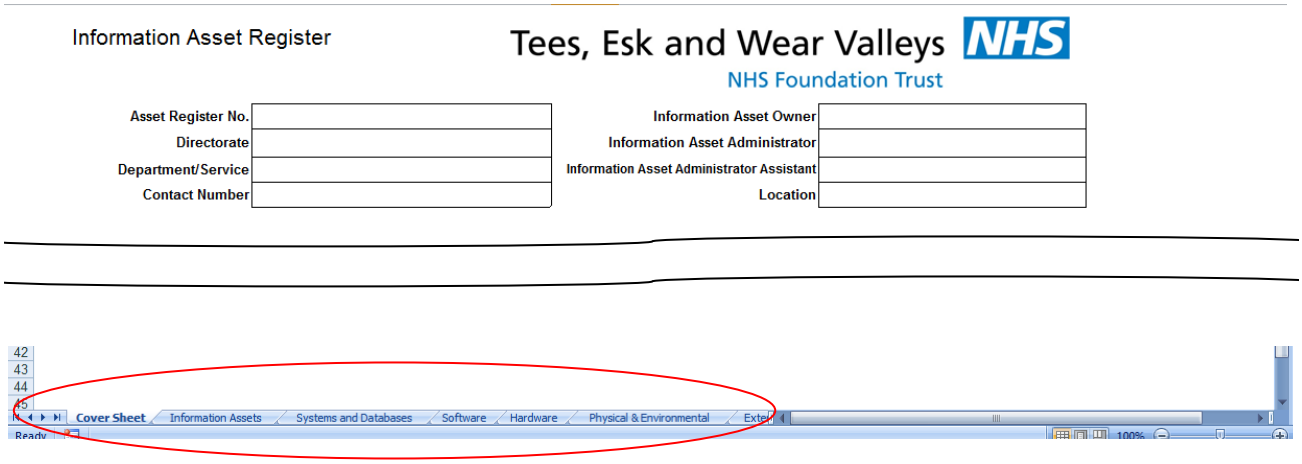
The Trust's position regarding information/data security and risk is reported annually to the SIRO by the Information Risk, Policy and Records Standards Manager. All monitoring and reporting documents are available to IAOs and IAAs for information.

3.8 Briefings

Briefings are the mechanism for communicating the latest developments, concerns and trends around information/data security and risk to the SIRO network.

4 What is an Information Asset Register?

IARs are created using Microsoft Excel and contain a number of worksheets:-



Tab	Description
Cover sheet	Shows the unique asset register number and who the IAO, IAA(s) IAAA(s) are. Also includes an overview review sheet to show who was the last to update the register and a brief description of the work done.
Systems and databases	Any paper or electronic systems used in your team that hold person identifiable information (patient and staff);
Software assets	Details of any software used within your team including any pre-installed software such as Microsoft Office. It is important to record licence numbers so that software can be restored if anything happens to the PC or laptop;
Hardware assets	Any hardware within the team that is used to store, process or move person identifiable or business sensitive information;
Physical and environmental assets	The means of keeping information assets secure and available e.g. access controls, air conditioning, Tambar unit, desk draw etc. If your team keeps paper patient records, make a note of the lock number on this tab. This helps when teams move and records need to be tracked and traced;
External services	Any third parties with whom the team shares information, identify where an information sharing agreement or contract exists;
Other	Any other assets that are important to your team but which do not fall into one of the above categories. This is additional information that provides the Trust with assurance that it is meeting its obligation to ensure confidentiality, integrity and availability of information and systems. This may include specialist staff, reputation and image, examples of local good practice e.g. training, awareness raising etc.

5 Maintaining an Information Asset Register

- Information asset registers are reviewed regularly by the IAO and IAA.
- The frequency of the review is determined by the risk rating of the asset, but will be at least once every 12 months or if processes change.

× **Do not delete** any information from your asset register. It is important that a full audit trail is kept when assets move or change.

If an asset is no longer used, or the information flow no longer happens:

✓ Highlight the row;

✓ Strike-through the text (press CTRL + Shift + F, then check the Strikethrough option);

✓ Complete the decommissioning details (the green columns on the right hand side of each worksheet).

5.1 Empty worksheets

Empty (blank) worksheets will be rated 'Red' in the annual risk report to the Senior Information Risk Owner.

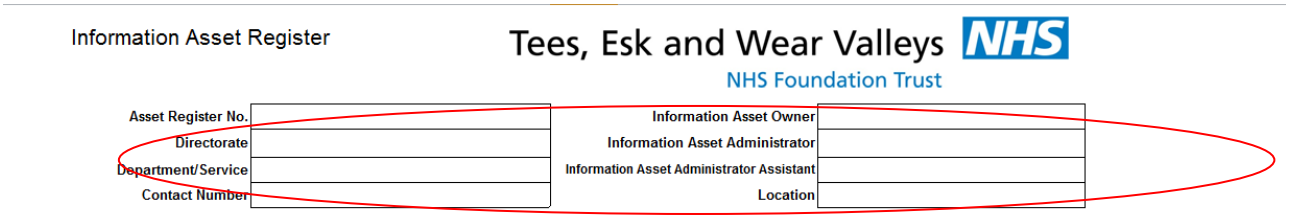
If there are no assets to add to a worksheet, add a note that "**This worksheet has been reviewed and there are no assets to record**" together with your name and the date.

5.2 Password protection

Your register may be protected by a password. This is to stop people accidentally updating the wrong register. It does not stop you opening and reading any register.

- If you can not remember your password, or have deleted the email since the password was sent to you, contact tewv.informationsecurity@nhs.net for a reminder.
- Do not create a copy of the register to avoid needing a password – duplicate registers cause confusion and increase risk of error when being maintained at a later date.

5.3 Cover sheet


Information Asset Register

Tees, Esk and Wear Valleys NHS
NHS Foundation Trust

Asset Register No.		Information Asset Owner	
Directorate		Information Asset Administrator	
Department/Service		Information Asset Administrator Assistant	
Contact Number		Location	

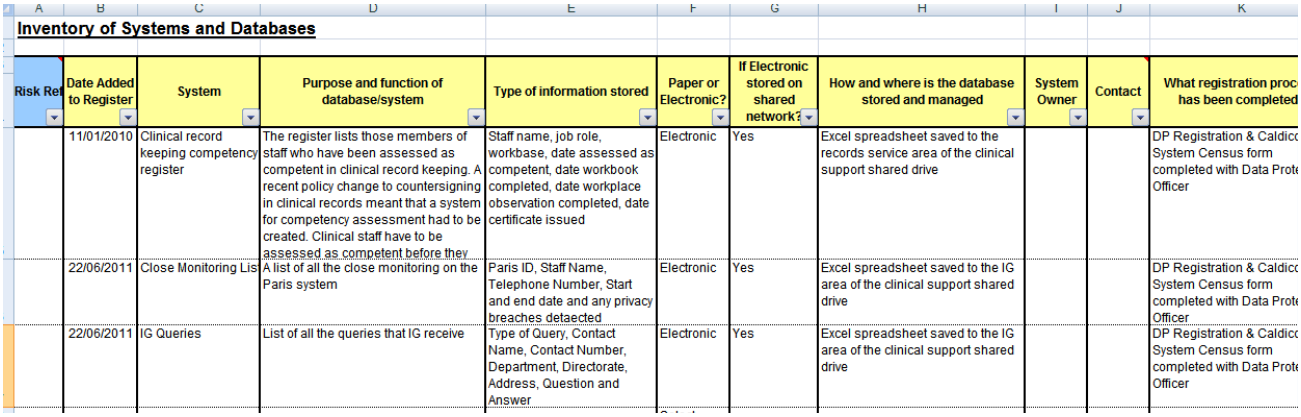
Step	Action
1	Check the details on the cover sheet are correct
2	Make any changes as needed
3	Notify any changes to IAO, IAA, IAAA or location to tewv.informationgovernance@nhs.net

5.4 Information assets

The use of this tab was withdrawn in July 2021. All information flows are now recorded centrally and form the Trust's Record of Processing Activity.

5.5 Systems and databases

It is a legal requirement that the Trust registers annually all systems and databases that are used to record person identifiable information. The information recorded on this worksheet is the means by which the Information Department's Compliance team knows which systems and databases need to be added to the annual registration.

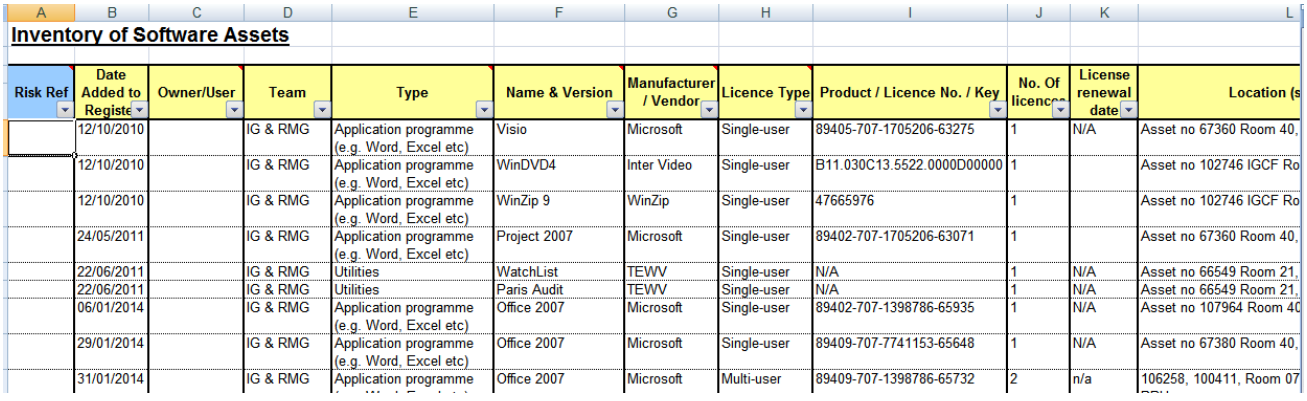

Inventory of Systems and Databases

Risk Ref	Date Added to Register	System	Purpose and function of database/system	Type of information stored	Paper or Electronic?	If Electronic stored on shared network?	How and where is the database stored and managed	System Owner	Contact	What registration proc has been completed
	11/01/2010	Clinical record keeping competency register	The register lists those members of staff who have been assessed as competent in clinical record keeping. A recent policy change to countersigning in clinical records meant that a system for competency assessment had to be created. Clinical staff have to be assessed as competent before they	Staff name, job role, workbase, date assessed as competent, date workbook completed, date workplace observation completed, date certificate issued	Electronic	Yes	Excel spreadsheet saved to the records service area of the clinical support shared drive			DP Registration & Caldicc System Census form completed with Data Prote Officer
	22/06/2011	Close Monitoring Lis	A list of all the close monitoring on the Paris system	Paris ID, Staff Name, Telephone Number, Start and end date and any privacy breaches detaected	Electronic	Yes	Excel spreadsheet saved to the IG area of the clinical support shared drive			DP Registration & Caldicc System Census form completed with Data Prote Officer
	22/06/2011	IG Queries	List of all the queries that IG receive	Type of Query, Contact Name, Contact Number, Department, Directorate, Address, Question and Answer	Electronic	Yes	Excel spreadsheet saved to the IG area of the clinical support shared drive			DP Registration & Caldicc System Census form completed with Data Prote Officer

Column	Description

Risk ref	Any high risk assets will need to be assessed to understand whether any mitigating actions need to be implemented and if the risk needs to be escalated (see section 7 – Risk Assessment of the Information Asset Register)
Date	The date the item was reviewed or added to the register.
System	A brief description of the system or database that holds the information, e.g. Referrals spreadsheet, paper diary etc.
Purpose and function of the database	The need for holding person identifiable information on a system or database must be justified
Type of information stored	A list of the types of information recorded
Paper or electronic?	Knowing whether the information is held electronically or on paper informs the risk assessment process
How and where the database is stored and managed	Paper records must be secured so that they are only accessed by authorised staff. Describe here how paper records are secured to prevent unauthorised access. Electronic information must be held on encrypted systems/devices that are owned by the Trust, e.g. shared drive. Describe here how electronic information is stored.
System owner/contact	Details of the person responsible for the system/database (usually the Information Asset Administrator)
What registration process has been completed?	Make a note if the system/database has been registered with Information Governance.
Any other relevant information	Any additional details that justify the need for the system/database and identify how it is protected.

5.6 Software



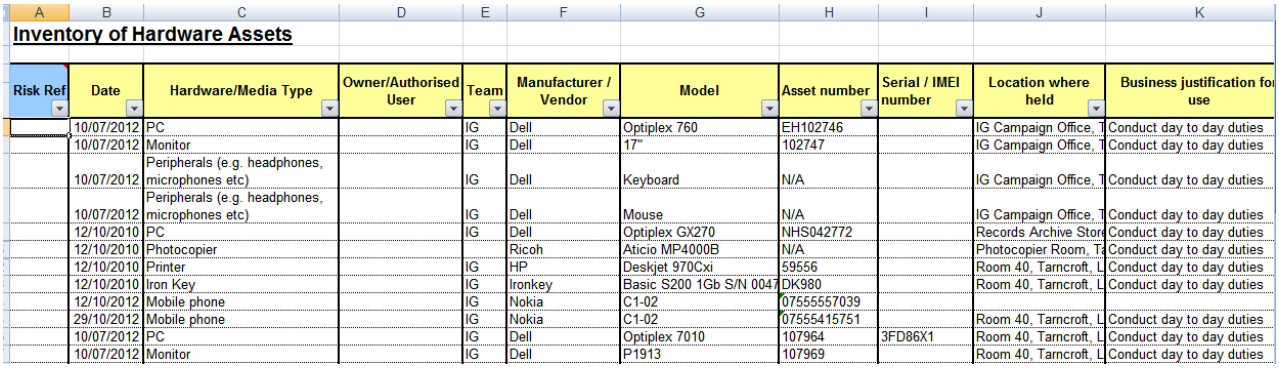
Inventory of Software Assets

Risk Ref	Date Added to Registe	Owner/User	Team	Type	Name & Version	Manufacturer / Vendor	Licence Type	Product / Licence No. / Key	No. Of licence	License renewal date	Location (s
	12/10/2010		IG & RMG	Application programme (e.g. Word, Excel etc)	Visio	Microsoft	Single-user	89405-707-1705206-63275	1	N/A	Asset no 67360 Room 40,
	12/10/2010		IG & RMG	Application programme (e.g. Word, Excel etc)	WinDVD4	Inter Video	Single-user	B11.030C13.5522.0000D00000	1		Asset no 102746 IGCF Ro
	12/10/2010		IG & RMG	Application programme (e.g. Word, Excel etc)	WinZip 9	WinZip	Single-user	47665976	1		Asset no 102746 IGCF Ro
	24/05/2011		IG & RMG	Application programme (e.g. Word, Excel etc)	Project 2007	Microsoft	Single-user	89402-707-1705206-63071	1		Asset no 67360 Room 40,
	22/06/2011		IG & RMG	Utilities	WatchList	TEWV	Single-user	N/A	1	N/A	Asset no 66549 Room 21,
	22/06/2011		IG & RMG	Utilities	Paris Audit	TEWV	Single-user	N/A	1	N/A	Asset no 66549 Room 21,
	06/01/2014		IG & RMG	Application programme (e.g. Word, Excel etc)	Office 2007	Microsoft	Single-user	89402-707-1398786-65935	1	N/A	Asset no 107964 Room 40
	29/01/2014		IG & RMG	Application programme (e.g. Word, Excel etc)	Office 2007	Microsoft	Single-user	89409-707-7741153-65648	1	N/A	Asset no 67380 Room 40,
	31/01/2014		IG & RMG	Application programme	Office 2007	Microsoft	Multi-user	89409-707-1398786-65732	2	n/a	106258, 100411, Room 07

Column	Description
Risk ref	Any high risk assets will need to be assessed to understand whether any mitigating actions need to be implemented and if the risk needs to

	be escalated (see section 7 – Risk Assessment of the Information Asset Register)
Date	The date the item was reviewed or added to the register.
Owner/User	The person who uses the software or is responsible for it
Team	The team the software belongs to
Type	The type of software asset – select from the drop down list
Name and version	The name that the software is known by and any version information, e.g. MSVisio 2010, WebICE , System One, Adobe Writer, BigHand, Autocad
Manufacturer/Vendor	The software manufacturer or the name of the firm that provided it, e.g. Microsoft, McKesson, Sunquest Information Systems, TPP etc.
Licence type	Select single-user or multi-user from the drop down if known
Product/Licence No/Key	It is important to record the licence number of your software. This will enable it to be restored should anything happen to the PC or laptop that stops the software working or being available. For information on how to find your licence number, see Appendix 1
No. of licences	Knowing how many licences are available within the Trust enables unused software to be redistributed to where it is needed and can save the Trust the cost of purchasing unnecessary software licences.
Location	The asset number of the PC or laptop the software has been installed on, and the physical location (e.g. room number, building, hospital) where the asset is used.
Business justification for use	This information is used to inform the risk assessment process, particularly when using software as a tool for recording person identifiable or business sensitive information.

5.7 Hardware



Inventory of Hardware Assets

Risk Ref	Date	Hardware/Media Type	Owner/Authorised User	Team	Manufacturer / Vendor	Model	Asset number	Serial / IMEI number	Location where held	Business justification for use
	10/07/2012	PC		IG	Dell	Optiplex 760	EH102746		IG Campaign Office, T	Conduct day to day duties
	10/07/2012	Monitor		IG	Dell	17"	102747		IG Campaign Office, T	Conduct day to day duties
	10/07/2012	Peripherals (e.g. headphones, microphones etc)		IG	Dell	Keyboard	N/A		IG Campaign Office, T	Conduct day to day duties
	10/07/2012	Peripherals (e.g. headphones, microphones etc)		IG	Dell	Mouse	N/A		IG Campaign Office, T	Conduct day to day duties
	12/10/2010	PC		IG	Dell	Optiplex GX270	NHS042772		Records Archive Store	Conduct day to day duties
	12/10/2010	Photocopier			Ricoh	Aticio MP4000B	N/A		Photocopier Room, Ta	Conduct day to day duties
	12/10/2010	Printer		IG	HP	Deskjet 970Cxi	59556		Room 40, Tarncroft, L	Conduct day to day duties
	12/10/2010	Iron Key		IG	Ironkey	Basic S200 1Gb S/N 0047	DK980		Room 40, Tarncroft, L	Conduct day to day duties
	12/10/2012	Mobile phone		IG	Nokia	C1-02	07555557039			
	29/10/2012	Mobile phone		IG	Nokia	C1-02	07555415751		Room 40, Tarncroft, L	Conduct day to day duties
	10/07/2012	PC		IG	Dell	Optiplex 7010	107964	3FD86X1	Room 40, Tarncroft, L	Conduct day to day duties
	10/07/2012	Monitor		IG	Dell	P1913	107969		Room 40, Tarncroft, L	Conduct day to day duties

Column	Description
Risk ref	Any high risk assets will need to be assessed to understand whether any mitigating actions need to be implemented and if the risk needs to

	be escalated (see section 7 – Risk Assessment of the Information Asset Register)
Date	The date the item was reviewed or added to the register.
Hardware/media type	Any hardware that is used to store, transfer, manipulate or work on information, such as PCs, laptops, mobile and smart phones, etc. Select from the drop down list.
Owner/authorised user	The name of the person that the hardware has been assigned to
Team	The team that the owner/authorised user works in
Manufacturer/vendor	The manufacturer or distributor of the hardware asset
Model	Refer to packaging or labelling on the asset to find any information that identifies the model
Asset number	Hardware that stores information must be purchased via Information Department and will be given an asset number which will be shown on a label on the asset. For Trust mobile phones, make a note of the telephone number
Serial/IMEI number	Refer to packaging or labelling to find the asset's serial number. To find the IMEI number of a mobile or smartphone, key *#06# on the handset.
Location where held	The physical location (e.g. room number, building, hospital) where the asset is used.
Business justification for use	This information is used to inform the risk assessment process, particularly when using hardware as a tool for recording or transferring person identifiable or business sensitive information.

5.8 Physical & environmental

Inventory of Physical & Environmental Assets

Risk Ref	Date	Asset Type	Additional Description (if required)	Owner/ Authorised User	Team	Location	Business justification for use	
	25/03/2015	Furniture	Filing cabinet- tall (Key 219)	Jane Drane	IG	D67, Tarncroft, LRH	for safe storage of confidential paper information	Los acc
	25/03/2015	Furniture	Filing cabinet-desk height (Key 292)	Theresa Parks	IG	D67, Tarncroft, LRH	for safe storage of confidential personnel files	Los acc
	25/03/2015	Furniture	Filing cabinet-tall (Key 380)	Theresa Parks	IG	D67, Tarncroft, LRH	for safe storage of confidential paper information	Los acc
	25/03/2015	Furniture	Under desk draw (Key 18187)	Louise Eastham	IG	D67, Tarncroft, LRH	for safe storage of confidential personnel files	Los acc
	25/03/2015	Furniture	Under desk draw (Key 18072)	Spare	IG	D67, Tarncroft, LRH	for safe storage of confidential personnel files	Los acc
	25/03/2015	Furniture	Under desk draw (Key 18003)	Jonathon Millington	IG	D67, Tarncroft, LRH	for safe storage of confidential personnel files	Los acc
	23/06/2014	Furniture	Shred-it confidential waste bin	Theresa Parks	Records	Medical Records office, RPH	For safe disposal of confidential waste. Key is held by Michael Pratt	Una con

Column	Description
Risk ref	Any high risk assets will need to be assessed to understand whether any mitigating actions need to be implemented and if the risk needs to be escalated (see section 7 – Risk Assessment of the Information Asset Register)
Date	The date the item was reviewed or added to the register.
Asset type	Select from the drop down list
Additional Description	Adding more detail about the item, e.g. desk side draw (Key 265) contains staff files,

6 Data Protection Impact Assessment

IAOs must ensure a Data Protection Impact Assessment has been carried out on Information Assets that might impact on people's privacy, e.g. the introduction of a system or database that holds person identifiable information.

For more guidance on introducing a system, see the Trust's policy and procedure for the introduction or upgrade of an information system. If you need help completing a Data Protection Impact Assessment, contact the Information Security Officer.

7 Risk Assessment of the Information Asset Register

With the exception of the Information Assets tab, whose risk assessment is determined by the IG Toolkit, the risk assessment process is exactly the same as for any other area of the Trust, i.e.

- Identifying, Assessing and Grading Risk
- Acceptability of Risk
- Calculating and Addressing Risk

This is documented within Appendix 8 of the Integrated Governance Strategy. Refer to the Integrated Governance Strategy for further guidance.

With regards to information/data risk, risk assessment considers potential impacts on the confidentiality, integrity and availability of systems and data, and the likelihood of those impacts occurring.

In assessing the appropriate level of security, account is taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed

The Trust-wide information asset register gives the risk ratings for information assets that are held and used to a set standard (i.e. Trust staff working in Trust premises). This means IAAs do not need to carry out risk assessments unless they and their team work differently

7.1 Completing a Risk Assessment Form

A risk assessment form is only completed when the risk to an information flow or asset has been assessed as High or the IAA/IAO considers it necessary that action is needed.

The form is used to show:-

- what risks you have identified from your information asset registers;
- what mitigating actions, if any, will be put in place;
- who will carry out these actions;
- when they will be completed.

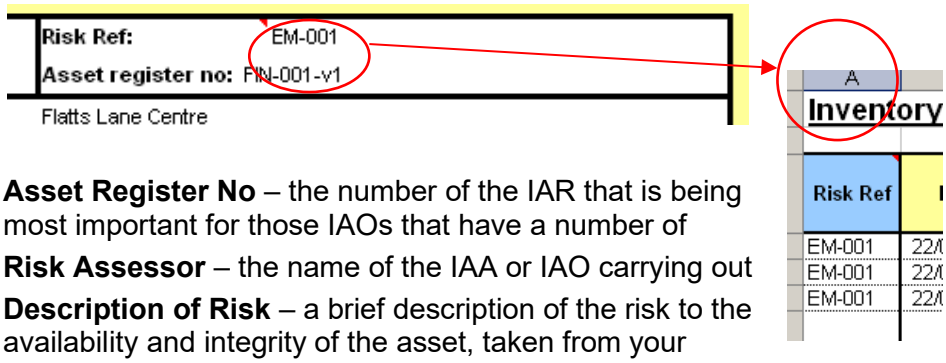
The risk assessment form also shows any risks that have been escalated by the IAO to a higher risk register.

Step	Action	Who
1	Open a blank risk assessment form. This can be found at:- T:\Information Risk Management\Blank Forms	IAA/IAO

2	Click File > Save As, saving a copy of the form to your Risk Assessment folder, e.g. T:\Information Risk Management\Information Asset Registers\Finance\Risk Assessment	IAA/IAO
3	Give your risk assessment form a meaningful description. A combination of the risk reference and description of risk (see below) works best, e.g. "EM-001 High Risk Outbound Emails"	IAA/IAO

7.2 Description of Risk Assessment Form

Risk Ref – create a reference number for the form. You need to add this reference to the risks being assessed on your IAR (see the example below). You can use the same risk ref for a number of information assets where they all have the same risk. For example, you can put all your high risk outbound emails on to one risk assessment.



Asset Register No – the number of the IAR that is being risk assessed. This is most important for those IAOs that have a number of registers;

Risk Assessor – the name of the IAA or IAO carrying out the risk assessment;

Description of Risk – a brief description of the risk to the confidentiality, availability and integrity of the asset, taken from your asset register, for example 'High risk outbound emails';

Information Asset – the description from your IAR, e.g. budget reports

Risk Rating Before – again from your IAR, e.g. High (information assets), 15 (Impact x Likelihood)

Risk Treatment – the measure that will be implemented to treat the risk:

- Accept = you can live with a particular risk without taking any action
- Reduce = action will be taken to reduce the risk to an acceptable level
- Transfer = share or shift the risk to where it can be more appropriately managed
- Avoid = stop the activity that causes the risk

Proposed Action – a description of the risk treatment, e.g. send using NHS.net

Person Responsible – the name of the person who will ensure the proposed actions are carried out. This may be different to the person carrying out the actions.

Escalate to Higher Risk Register? – the need for escalation is determined by the risk rating. Refer to the Integrated Governance Framework to decide whether the risk needs to be logged on Datix and escalated.

8 Requesting a New Information Asset Register

This will only be required if a new team is created or existing teams merge and their individual registers are archived.

New registers can be requested by the IAO or their nominated IAA.

Step	Action	Who
1	Open the New Information Asset Register form via the IG pages on InTouch:- Intouch > Services > Clinical Support Services > Information Governance > Documents	IAA/IAO
2	• Click File > Save As • Rename the document New Information Asset Register [Insert Directorate_Team Name] • Save it to the Governance folder on your shared drive.	IAA/IAO
3	Complete the questions following the instructions on the form and giving as much detail as possible	IAA/IAO
4	Save the form when finished	IAA/IAO
5	Email the form to the Information Security mailbox:- tewv.informationsecurity@nhs.net	IAA/IAO

9 Disposing of an Information Asset Register

This is required if:-

- a team is to be disbanded; or
- more than one team is being merged and the old registers are to be archived.

Only the Information Asset **Owner** can submit an Information Asset Register Disposal form.

The Information Security team should be contacted for advice before submitting the disposal form (tewv.informationsecurity@nhs.net)

Step	Action	Who
1	Open the Information Asset Register Disposal form either from your Blank Forms folder on the t:/ drive or from the Information Governance pages of InTouch:- Intouch > Services > Clinical Support Services > Information Governance > Documents	IAA/IAO
2	• Click File > Save As • Rename the document Information Asset Register [Insert Directorate_Team Name_IAR Ref] • Save it to the Governance folder on your shared drive.	IAA/IAO
3	Complete the questions following the instructions on the form and giving as much detail as possible	IAA/IAO
4	Save the form when finished	IAA/IAO

5	Email the form to the Information Security mailbox:- tewv.informationsecurity@nhs.net	IAA/IAO

10 Changing an IAO or IAA

Changes to an information asset owner or administrator must be notified to the Information Department's compliance team via email to tewv.informationsecurity@nhs.net

Changes should be notified at the time they become known to enable the Compliance team to be aware of the handover of assets and registers and provide advice and assistance if needed.

11 Teams moving to new premises

Teams who are moving from one building to another have an obligation to track and trace **all** their information assets. Refer to the Commissioning Team Action Plan that you receive from the Capital Projects Officer who is supporting your move.

12 Definitions

Term	Definition
Information Assets	Those that are central to the efficient running of departments of the Trust, for example patient, finance, stock and staff data. They also include the systems, hardware and software that are used to process and store this data.
Information Asset Register	Information assets should be documented in an asset register. There is one asset per team, maintained by an Information Asset Administrator (IAA) under the management supervision of an Information Asset Owner (IAO).
Overarching Information Asset Register	Effectively a 'register of registers' showing who owns and administrates each register to enable tracking. It does not duplicate any information that is held in the actual registers.
IAA	Information Asset Administrator
IAAA	Information Asset Administrator Assistant
IAO	Information Asset Owner
IAR	Information Asset Register
IG	Information Governance
PII	Person Identifiable Information
SIRO	Senior Information Risk Owner
TNA	Training Needs Assessment or Training Needs Analysis

12.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
IAOs/IAAs	Workshop (face-to-face or virtual)	2 hours	Annually
SIRO	Online SIRO training via IG Toolkit	1 hour	On appointment

13 How the implementation of this procedure will be monitored

The Trust is in the process of implementing centralised asset management which will remove much of the manual maintenance of information asset registers. The continued requirement for this procedure will therefore be reviewed as part of the centralised asset management project.

14 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval:	08 December 2021	
Next review date:	08 December 2024	
This document replaces:	IT-0010-001-v1 Information Asset Register Procedure	
This document was approved by:	Name of committee/group	Date
	Heads of Information	15 July 2021
This document was ratified by:	Name of committee/group	Date
	Digital Performance and Assurance Group	08 December 2021
An equality analysis was completed on this document on:	05 July 2021	
Document type	Public	

Change record

Version	Date	Amendment details	Status
1			Withdrawn

1(1)	Mar 2014	Added instructions on how to maintain individual worksheets on the asset register following a review of the Trust's information risk systems.	Withdrawn
1(1)	Jan 2017	Review date extended 12 months	Withdrawn
1	Feb 2018	Procedure renumbered from CORP/0056/v1(1) to IT-0010-001-v1 to reflect that this procedure sits under the Information Security and Risk Policy Reviewed in line with GDPR: Privacy Impact Assessment renamed Data Protection Impact Assessment Section 7 extended re risk assessment process Section 11 added re teams moving premises Amendments to job title throughout	Withdrawn
	July 2020	Review date extended 6 months	Withdrawn
2	08 Dec 2021	Full review which wording changes throughout. Information mapping amended to indicate information flows are captured in Record of Processing Activities. References to changes arising from centralised asset management added to document.	Published

Appendix 1 - Equality Analysis Screening Form

Please note; The Equality Analysis Policy and Equality Analysis Guidance can be found on InTouch on the policies page

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc.	Information Department					
Policy (document/service) name	Information asset register procedure					
Is the area being assessed a…	Policy/Strategy		Service/Business plan		Project	
	Procedure/Guidance			X	Code of practice	
	Other – Please state					
Geographical area covered	Trust-wide					
Aims and objectives	The purpose of this document is to provide guidance on:- • Populating and maintaining information asset registers; • Requesting a new asset register; • Disposing of and archiving asset registers; • Treating and managing risk via the Information Asset Risk Assessment form.					
Start date of Equality Analysis Screening	05 July 2021					
End date of Equality Analysis Screening	05 July 2021					

You must contact the EDHR team if you identify a negative impact.

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?

The procedure benefits all individuals and organisations whose sensitive and personal information the Trust holds, transfers or processes

2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?

Race (including Gypsy and Traveller)	No	**Disability** (includes physical, learning, mental health, sensory and medical disabilities)	No	**Sex** (Men, women and gender neutral etc.)	No
Gender reassignment (Transgender and gender identity)	No	**Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.)	No	**Age** (includes, young people, older people – people of all ages)	No
Religion or Belief (includes faith groups, atheism and philosophical belief's)	No	**Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave)	No	**Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners)	No

Yes – Please describe anticipated negative impact/s

No – Please describe any positive impacts/s

Following the procedure will impact positively as this will ensure the security of information relating to individuals, including sensitive information the Trust may hold relating to a person's protected characteristic(s)

3. Have you considered other sources of information such as; legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.? **If 'No', why not?**	**Yes**	**X**	**No**	

Sources of Information may include: • Feedback from equality bodies, Care Quality Commission, Equality and Human Rights Commission, etc. • Investigation findings • Trust Strategic Direction • Data collection/analysis • National Guidance/Reports	• Staff grievances • Media • Community Consultation/Consultation Groups • Internal Consultation • Research • Other (Please state below) **NHS Digital**

4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Gender, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership
Yes – Please describe the engagement and involvement that has taken place
Trust-wide consultation when developing the procedure
No – Please describe future plans that you may have to engage and involve people from different groups

5. As part of this equality analysis have any training needs/service needs been identified?					
No	Please describe the identified training needs/service needs below				
A training need has been identified for;					
Trust staff	No	Service users	No	Contractors or other outside agencies	No
Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so					
The completed EA has been signed off by: You the Policy owner/manager: Type name: Andrea Shotton				Date: 05-Jul-2021	
Your reporting (line) manager: Type name: Lorraine Sellers				Date: 05-Jul-2021	
If you need further advice or information on equality analysis, the EDHR team host surgeries to support you in this process, to book on and find out more please contact the team.					

Appendix 2 – Approval checklist

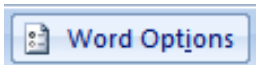
	Title of document being reviewed:	Yes/No/ Not applicable	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	N/A	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	N/A	
	Are key references cited?	N/A	
	Are supporting documents referenced?	N/A	
6.	**Training**		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	
7.	**Implementation and monitoring**		

	Title of document being reviewed:	Yes/No/ Not applicable	Comments
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
10.	**Publication**		
	Has the document been reviewed for harm?	Yes	
	Does the document identify whether it is private or public?	Yes	
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	N/A	

Appendix 3 – How to find your Microsoft licence number

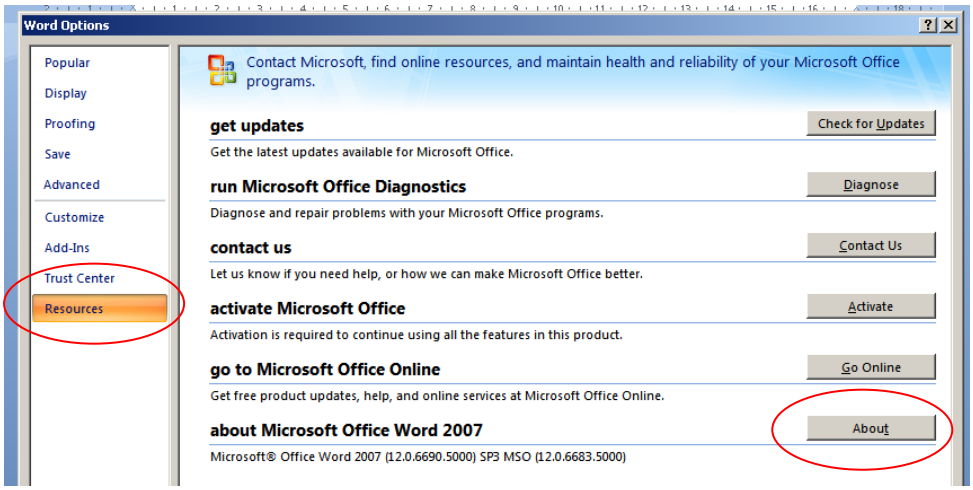
1> Click the Microsoft Office Button

2> Select Word Options



3> Click Resources

4> Click About



5> The licence number is displayed