**POLICY**

# Information Asset Owners (IAOs)

| | | | |
|---|---|---|---|
| Owning Department: | Information Compliance | | |
| Department SPOC: | | | |
| CPU Lead: | | | |
| Risk Rating: | Low | Legal Sign Off:<br>Date: | Yes<br>20/01/16 |

## Approved by

| | | | |
|---|---|---|---|
| JNCC: | 04/01/2016 | | |
| Published Date: | 23/10/2018 | Review Date: | 23/10/2022 |

## Index



### Legal Basis

*(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.*

***Legislation/Law specific to the subject of this policy document***

| ***Section*** | ***Act (title and year)*** |
|---|---|
| | Common law duty of confidentiality |

***Other legislation which you must check this document against (required by law)***

| ***Act (title and year)*** |
|---|
| Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination) |
| Equality Act 2010 |
| Crime and Disorder Act 1998 |
| Health and Safet at Work etc Act 1974 and associated regulations |
| General Data Protection Regulation and Data Protection Act 2018 |
| Freedom Of Information Act 2000 |
| Common law duty of confidentiality |
| Computer Misuse Act 1990 |
| Copyright, Designs and Patents Act 1988 |
| Criminal Procedure and Investigations Act 1996 (CPIA) |
| Protection of Freedoms Act 2012 |
| Regulation of Investigatory Powers Act 2000 (RIPA) |

### Other Related Documents

- Information Management Policy
- Data Protection Policy
- Freedom of Information Policy

- Information Security Policy
- Records Management Policy
- Information Sharing Policy
- Information Risk Management Policy
- Force Risk Appetite Statement
- Data Quality Policy
- Privacy Impact Assessment Policy
- Information Audit and Monitoring Procedure
- Information Asset Owners Guide
- College of Policing APP (Authorised Professional Practice) Management of Police Information
- Home Office (2005) Code of Practice on The Management of Police Information

## 1. Policy Aim

1.1 This policy sits under the Information Management Policy.

1.2 The aim of this document is to provide Information Asset Owners (IAOs) with information that promotes the maintenance of good practice and compliance with the Data Protection Act 2018. It is a means by which the processing of both Norfolk and Suffolk Constabularies' information assets meets the requirements of the College of Policing Authorised Professional Practice (APP) on Information Management and the Home Office (2005) Code of Practice on The Management of Police Information (MoPI).

## 2. Purpose

2.1 The purpose of this policy is to advise IAOs of the responsibilities of the role and provide assistance with the effective and appropriate management of information by giving recommendations on:

- Identifying Information Assets
- IAO Responsibilities
- How to Achieve Responsibilities
- Managing Information Risks
- Training and Resource

## 3. Applicability

3.1 Adherence to this policy should be observed by all Norfolk and Suffolk personnel designated as an Information Asset Owner.

## 4. What is an Information Asset?

4.1 An information asset is a body of information, defined and managed as a single unit so that it can be understood, shared, protected and exploited effectively. The term 'information asset' covers a wide meaning and includes but is not limited to files, operational orders, briefing sheets, plans, maps, reports, photographs, tapes, discs and electronic data records.

4.2 The asset could include both sensitive personal information and non-personal information that is critical to the business and could be held in paper as well as electronic formats. An asset could be a single significant document or a set of related data, documents or files. The asset can be shared or confined to a specified purpose or organisational unit.

## 5. Identifying an Information Asset

5.1 IAOs should identify all information processed within a department, group them together into manageable portions, then group together the types of information processed (i.e. spreadsheets, project plans etc), including both manual and computerised systems.

5.2 Once categorised by type, use the broad definitions of value, risk, content and lifecycle to assess the role of the asset within the department and consider the level of granularity required. Targeted questions can be asked to identify an asset:

Value

- Does it have a value to the Constabularies?
- Would there be any legal, financial impact or damage to reputation if the information could not be generated?
- If the information could not be accessed easily, would this effect operational efficiency?
- What would be the consequences of not having this information?

Risk

- Is there a risk associated with the information?
- Is there a risk of losing the information?
- Is there a risk that the information is inaccurate?
- Is there a risk that the information could be altered without consent to do so?
- Would there be any risks arising from inappropriate disclosure?

Content

- Does the information have a specific purpose and content?
- How is the information comprised and what is it comprised of?
- Does the use of the information meet the specified purpose?

- Does the content relate to any other groups of information in any other business areas?

Lifecycle

- Does the information have a manageable lifecycle? E.g. from inception, to everyday use, any requirements for change and potential obsolescence.
- Have all the different aspects of the group of information been created for a common purpose?
- Will all the components be disposed of in the same way and according to the same rules?

5.3 A database is a clear example of a single information asset. Each entry in the database does not need to be treated separately; the information can be grouped together as one information asset. All the information within the asset will have comparable risks (i.e. data quality, monitoring and inspection, retention and deletion).

5.4 All files associated with a single project can be considered a single asset. This may include emails to and from project staff, spreadsheets, project plans etc. The information will have the same risks associated with it however, further levels of granularity may need to be introduced to manage each definable process more efficiently.

5.5 Assets can contain other assets. With the introduction of further granularity, clear rules must be defined about how the management and retention of information is maintained at different levels.

## 6. Information Asset Owner Responsibilities

6.1 The role of the IAO is about managing information, not systems.

6.2 The IAO is responsible for ensuring that information assets are handled and managed appropriately. An IAO is appointed by, and reports to, the Senior Information Risk Owner (SIRO) and will support this role with its overall information risk management function. As such IAOs will be senior/ responsible individuals involved in the running of the relevant business area(s).

6.3 In order to meet the responsibilities of the role, an IAO must:

- Promote a culture that values, protects and uses information for the success of the Constabularies and the public good.
- Be aware of what information the asset holds, and what data travels in or out.
- Know which roles have access to the information and why, and monitor usage to confirm policies are being complied with.
- Ensure the asset is fully used to its maximum benefit, identifying any information sharing opportunities and transparency requirements and recognise requests for disclosure of data.
- Manage and understand potential risks to the asset, provide assurance to the SIRO and make certain any data loss incidents are appropriately addressed.

6.4 The role necessitates an appreciation and understanding of different functions within the organisation and, where required, bringing together the activities of others who have specialist areas of responsibility. Information Compliance, Information Security, Records Management and ICT are all key points of reference providing support to IAOs.

6.5 IAOs can delegate different areas of responsibility to individuals. Commonly referred to as Information Asset Administrator's (IAAs), these individuals are usually operational members of staff who understand and are familiar with the Information Asset within their business area. The IAA will ensure that local policies and procedures are followed, recognise actual or potential security incidents, consult with the IAO on incident management issues and ensure that the day-to-day effective administration of the information asset is maintained.

6.6 If responsibility is delegated, IAOs must ensure that the process is properly supervised and that clear reporting lines are in place in order that the IAO maintains awareness of the status of the information asset.

6.7 The IAO will retain overall responsibility of the information asset and the SIRO will retain accountability for proper information management and handling.

6.8 Carrying out the role of an IAO efficiently can deliver considerable advantages. It can provide a coherent and clear-cut understanding of the information held and help to establish the value of the information, its sensitivity, the levels of dependency on the information retained and who is accountable. It will enable an IAO to operate transparently and responsibly, improving public confidence and service.

6.9 IAOs are responsible for processes including security, related to their Information Asset. The introduction and continued operation of information assets is a business driven process that must be managed. For a definition on 'processing' refer to the Data Protection Policy.

How to Achieve Responsibilities

6.10 Some of the responsibilities of an IAO will require constructive action, and some will require monitoring tasks being undertaken by others. The following will assist in making sure all responsibilities are met:

| **Promote a culture which values, protects and uses information for the success of the Constabularies and the public good** | |
|---|---|
| What needs to be done | How to achieve this |
| • Complete the IAO training package.<br>• Check that the handling of information assets complies with the Data Protection Act 2018, the Freedom of Information Act 2000 and the Constabularies' compliance procedures and policies.<br>• Establish and record the business value of the information asset(s). | • Learning packages on NCALT (National Centre for Applied Learning Technologies) and IAO workshops.<br>• Train the staff that use the information asset(s) in their duties and responsibilities under the relevant Acts (via NCALT packages) and ensure they are putting them into practice. Consider using PDR objectives to achieve this.<br>• Provide guidance to those who use the information asset(s) as to the rules of use and the consequences of non-compliance.<br>• Talk to the Joint Information Management Strategic Board (JIMSB) and SIRO about ways that can assist with any proposed culture changes.<br>• Record any 'lessons learned' to enable the review of policies/ procedures and make appropriate changes to departmental or Constabulary practices.<br>• Contact Information Security to discuss appropriate physical, procedural and personnel security.<br>• Contact the Information Management Dept; in particular the Data Protection and Freedom of Information teams to establish if the way in which the information asset(s) is handled meets the requirements of the Acts. |

| Be aware of what information the asset holds, and what data travels in or out | |
|---|---|
| What needs to be done | How to achieve this |
| • Understand who has access to the information asset(s) and why, and monitor use.<br>• Establish whether any other parties or outside agencies rely on the information to deliver a service and understand how information is managed to achieve this purpose.<br>• As far as possible, approve and minimise transfers of non-personal and personal information.<br>• Implement procedures to minimise and protect any information transferred to removable media.<br>• Monitor the transfer of non-personal and personal information to removable media.<br>• Be aware of any requests for information received and consider if the service to the public could be enhanced through greater access to information contained within the asset(s).<br>• Consider the risks to the information asset(s) by understanding the content of the information, its purpose and how any transfer of information is managed. | • Keep a record of who has access to the information asset(s) and at which level i.e. administrator, editor, reader.<br>• Regularly review the list of 'active' users and disable accounts that are no longer required.<br>• Document the detail of the information asset(s) e.g. content of the information, protective markings applied, type of information retained (personal/ non-personal), processes for monitoring data quality, value of the asset to the organisations, retention and disposal guidelines. Please contact the Compliance Officer for further assistance in documenting the detail.<br>• Apply version controls to enable monitoring of any changes.<br>• Liaise with the Information Sharing Officer for advice on how to manage agreements on the sharing of personal information between parties.<br>• Contact Information Security for further advice about the practicalities of ensuring the safety of the information asset(s) and data loss prevention.<br>• Ensure that each asset is recorded on the Information Asset Register. Contact the Compliance Officer for further assistance. |

| Know which roles have access to the information and why, and monitor use to confirm policies are being complied with | |
|---|---|
| What needs to be done | How to achieve this |
| • Know who has access to the information asset(s) and why, and monitor use.<br>• Introduce guidelines for users of the asset and stipulate conditions for use. | • Be familiar with the policies and procedures that govern how to use the asset.<br>• Regularly review any guidelines or policies issued to ensure they are fit for purpose.<br>• Keep a record of who has access to the information asset(s) and at which level i.e. administrator, editor, reader etc.<br>• Consider if access should be role dependent and establish a set of rules in respect of how access is authorised.<br>• Regularly review the list of 'active' users and disable accounts that are no longer required. Ensure that clear processes are in place to advise users how to request access and how to notify that |

| | |
|---|---|
| | access is no longer required.<br>• Engage with the Compliance Auditors for advice re: monitoring the correct use of the asset(s). |

| **Ensure the asset is used to its maximum benefit, identifying any information sharing opportunities, transparency requirements and recognise requests for disclosure** | |
|---|---|
| What needs to be done | How to achieve this |
| • Explore formal Information Sharing arrangements to safeguard against inappropriate disclosure of information.<br>• Recognise requests for disclosure of information and log these requests.<br>• Consider regularly how better use could be made of the information asset(s) within the law.<br>• Where it is decided that public access to information is in the public interest, this should be reflected within the Freedom of Information Publication Scheme to comply with transparency requirements. | • Liaise with the Information Compliance team for best practice guidance on how to recognise and deal with information requests. Establish if the response is 'business as usual' or if specialist assistance is required from another department (i.e. Freedom of Information/ Data Protection teams).<br>• Liaise with the Freedom of Information team for best practice guidance on how to recognise requests for public information and advice on whether consideration should be given for inclusion of datasets within the Publication Scheme.<br>• Consider creating a log of requests received specifying the type of information required and what action was taken. This will better inform future applications of a similar nature and help monitor the systematic disclosure of the same types of information.<br>• Liaise with the Information Sharing Officer for advice on how to manage agreements on the sharing of information. |

| Manage and understand potential risks to the asset, provide assurance to the SIRO and make certain any data loss incidents are appropriately addressed | |
|---|---|
| What needs to be done | How to achieve this |
| • Be familiar with the requirements of the Corporate and Department Risk Registers, the Information Risk Management Policy and Force Risk Appetite Statement.<br>• All risk decisions should be taken demonstrably in accordance with the Information Risk Management Policy and the Risk Appetite Statement. If a risk is outside of the risk appetite then it must be escalated to the SIRO for a decision on whether to accept the risk, invest in mitigating the risk or avoid the risk.<br>• Where users raise concerns that undertaking a course of action will place the information asset(s) and therefore the department or force at risk, make appropriate decisions as necessary ensuring that others are consulted as required and document the reasons to support the decision.<br>• Contribute to the department's risk assessment. Her Majesty's Inspectorate of Constabulary (HMIC) requires information compliance audits to be conducted and in particular, High Risk assets are risk assessed on an annual basis – ensure participation in the process to be better informed as to the information compliance risks to the asset(s).<br>• Establish what the risks are to the asset(s) e.g. when personal information is moved between organisational units and/ or partner agencies.<br>• Ensure controls are effective to mitigate any risks. | • Be aware of all the potential risks to the information asset(s).<br>• Read the Force Risk Management Policy. This will provide useful information about the different areas of risk; which are likely to have the most significant impact and point to where the focus of risk management should be in relation to the asset(s).<br>• Look at the different mediums of how the information asset(s) is managed i.e. –<br>o Databases – who has access and what personal information is held? Are all databases managed in a consistent manner? If not, what are the variances that dictate the different handling requirements?<br>o Information stored on shared drives – who has access to information asset(s) on shared drives and why? What personal information is stored in this location and what security arrangements are in place for protecting it?<br>• Establish the requirements to be able to use the asset(s) and utilise this information to assess risks and opportunities:-<br>o Identify the management processes and equipment needed to fulfil requirements.<br>o What technology is relied upon to maintain operational use of the asset(s)?<br>o Are there any risks that arise from changes to the organisation? Technological advances? Disclosure of information?<br>• Place all significant risks to the information asset(s) on the Information Risk Register.<br>• Talk to the JIMSB and SIRO about how risk policies apply to the information asset(s).<br>• Provide regular written updates to the JIMSB and SIRO in respect of the use and security of the asset(s). |

Managing Information Risks

6.11 Identify which areas of business are susceptible to risk and put processes in place to mitigate any potential weaknesses and minimise the impact should data loss occur. IAOs must guard against:

- Inappropriate access to, or disclosure of, personal, non-personal and protectively marked data by personnel, contractors and outside agencies, whether knowingly or accidentally.
- Poor quality of information and poor quality assurance.
- Information loss – IAOs should be mindful of how data is handled particularly during its transfer or movement, or as a result of business change which may cause a loss of immediate access to information.
- Loss of digital continuity i.e. the lifespan of an information asset; how long its use and retention is required, is often different to the lifespan of the ICT system that is used to access the information. Remember, information is not the same as ICT systems – ICT systems are the platforms on which information is managed.
- Weak change management – business needs change, systems change and the risks may change. Policies and procedures must be kept up to date accordingly.

6.12 In order to effectively manage exposure to information risk, there are several measures that IAOs can consider:

Roles

- Know who the Senior Information Risk Owner (SIRO) is within both Norfolk and Suffolk Constabularies.
- Identify the Information Asset Owner (IAO).
- Appoint Information Asset Administrators (IAAs) to assist with the responsibilities of the IAO function.
- Keep records of who has access to personal and non-personal data and at what level.

Maximising Benefit

- Continually review how better use could be made of the information asset within the law.
- Actively look to publish information within the Freedom of Information Publication Scheme.

Information Management & Integrity

- Establish what information assets exist within the business area and in which formats.

- Ensure that the information is proportionate to the purpose for which it was acquired and kept for no longer than is necessary.
- Ensure that information is accurate and up to date.
- Understand what happens to the asset at each stage in its lifecycle.
- As business needs change, plan for the potential impact this may have on information i.e. information may be corrupt or illegible with technological advances.
- Comply with all statutory and regulatory requirements.
- Follow best practice in information and records management.
- Explore formal Information Sharing arrangements to safeguard against inappropriate disclosure of information.

Review

- Conduct at least an annual assessment of information risk.
- Share and discuss the information with the JIMSB/ SIRO.

Governance and Culture

- Foster a culture that values, protects and uses information for the good of the Constabularies and the wider public.
- Encourage comprehensive policies and controls in respect of the asset(s) and ensure these are reviewed regularly.
- Ensure that lessons are learnt should things go wrong.
- Reflect performance in managing risk in PDRs.
- Establish ways for individuals to feel confident in reporting information risks to senior management and then demonstrate that action is taken in response.

Incident Management

- Follow the Information Security Policy for reporting, managing and recovering from information risk incidents.
- Define responsibilities and make personnel aware of the Information Management policies.

Transparency

- Publish an information strategy in relation to the asset(s) setting out how data should be handled and how to address any concerns. IAOs are to ensure the asset strategies link in with the Forces' Information Management Strategy.

## 7. Information Asset Register

7.1 An Information Asset Register (IAR) is a tool for understanding and managing the information assets of both Norfolk and Suffolk Constabularies and can be used to identify areas of potential risk to the asset. By understanding the nature of the information held, an IAO can mitigate the risks more easily.

7.2 The Joint Norfolk and Suffolk Constabularies IAR records the purpose of the asset, location, type of information held, security arrangements related to the asset, any links the asset has to other areas of the organisation, together with details on the Information Asset Owner and Administrator.

7.3 Any major changes to information assets must be notified to the Compliance Officer for inclusion on the IAR. This includes new and or replacement software listed on the IAR, updates and installations, removal or archiving of an information asset and the creation of a new information asset.

7.4 A Data Protection Impact Assessment should be carried out whenever a new process or information asset is likely to involve a new use or significantly change the way in which personal data is handled.

## 8. Data Protection Impact Assessments

8.1 A Data Protection Impact Assessment (DPIA) is a flexible process, which will enable both Norfolk and Suffolk Constabularies to systematically and accurately identify and minimise the privacy risks of new policies, initiatives and projects while allowing the aims of the project to be met whenever possible.

8.2 A DPIA can be carried out for any project which involves the use of personal data, or to any other activity which may have an impact on the privacy of individuals. DPIAs are employed for new projects as this allows a greater scope for influencing how the project will be applied but should also be considered for revisions of existing projects. An IAO may be required to conduct a DPIA or have involvement in the process if the initiative has an effect on an asset.

8.3 A DPIA should start in the initial stages of a project e.g. at project initiation phase or its equivalent or the business case stage. When it is apparent that a project will have some level of impact on privacy, IAOs should start to consider how these issues will be addressed.

8.4 For further information about the process, please refer to the Data Protection Impact Assessment Policy and/ or contact the Compliance Officer for assistance.

## 9. Manage Data Loss and Breaches

9.1 With the progression of technological advances and the development of policies, Norfolk and Suffolk Constabularies have become more dependent on the use of information assets for the delivery of services as well as strategic and administrative functions. To continue the successful operation of services and assurance, there is a need for a high standard and consistent approach to information security across both organisations.

9.2 Information is a valuable asset and everyone, not just IAOs are responsible and accountable for protecting it. The core functions of the Constabularies rely upon information and the loss, corruption or destruction of information, whether accidentally or maliciously, is likely to impact on policing services.

9.3 There are three basic components of Information Security:

- Confidentiality – ensuring that information is accessible only to those authorised to have access.
- Integrity – safeguarding the accuracy and completeness of information and processing methods.
- Availability – ensuring that authorised users have access to information when required.

9.4 The effective handling of these areas should enable IAOs to guard against data loss. However, an IAO must recognise when data loss occurs, or has the potential to occur, and manage incidents accordingly.

9.5 Incidents can generally be described as an adverse event which has led, or could lead, to a breach of policy, security, confidentiality, legislation or regulation. They can be caused deliberately or accidentally; whatever the case, they should be reported.

9.6 An information security incident is the suspected failure in security (not solely restricted to information stored electronically) that could potentially affect confidentiality, integrity or availability. Incidents will typically involve the improper disclosure of information from an information asset, unauthorised access to an information asset and using inappropriate methods to transmit protectively marked data.

9.7 Reporting security incidents is essential to identifying:

- Weaknesses in systems and products
- Policies and processes that require review/ revision
- Education and awareness training that requires review/ revision
- The need to alert other users potentially affected.

9.8 All information security incidents must be reported to the Information Security team via the Security Incident forms as soon as discovered.

9.9 Under the new Data Protection legislation, the Constabularies have an obligation to report data breaches that result in high risk to an individuals' rights and freedoms to the Information Commissioner's Office within 72 hours.

## 10. Disclosure of Information

10.1 Data sharing across and between organisations can play an important part in providing a better, more efficient service to customers however the disclosure of information must be carried out only when it is appropriate to do so.

10.2 Good practice recommendations will assist in the gathering and sharing of information in a way that is fair and transparent and in line with the rights and expectations of the parties whose information is being shared.

10.3 Information sharing can take the form of:

- A mutual exchange of data.
- One or more organisations providing data to a third party or parties.
- Systematic, routine information sharing where the same groups of data are shared between the same organisations for an established and legal purpose.

10.4 The term 'data sharing' broadly refers to the disclosure of data from one or more organisation(s) to other third party organisations/ partner agencies or the sharing of data between different parts of the organisation.

10.5 Some data sharing won't involve disclosing information that is personal to individual's, e.g. statistical records, however an IAO must identify those data sets which if released, could cause harm or distress to an individual.

10.6 If it is decided that it is productive to enter into an arrangement with another party to share information, an IAO should identify the objective(s) that the exercise is meant to achieve, consider the potential benefits and risks and assess the likely outcome of not sharing the information. Bear in mind the following:

- What is the sharing meant to achieve?
- What information needs to be shared?
- Who requires access to the shared information?
- When and how should it be shared?
- Are there any risks to the sharing of information?
- Can objectives be achieved without sharing information or by anonymising the data?

- Is consent required?

10.7 It is good practice to review any arrangements in place periodically, particularly where information is shared on a large scale or on a regular basis.

10.8 IAOs should refer to the Information Sharing Policy for further guidance and/ or contact the Information Sharing Officer.

## 11. Training and Resource

11.1 All personnel are reminded of the Information Management Computer-Based Training (CBT) package available via NCALT.

11.2 IAOs must ensure that all new starters successfully complete the Information Management CBT package as well as any external individuals who have access to police information systems.

11.3 IAOs must ensure that all current personnel complete the package every two years. It is good practice to include completion of the modules as a PDR objective and ensure that the package is successfully completed within the set timescale.

11.4 IAOs are encouraged to engage with the Information Management department who can provide specific advice and training about the responsibilities of the role.

## 12. Who to Contact about this Policy

12.1 Questions regarding this policy and its operation should initially be referred to the Compliance Officer on behalf of the Head of Information Management:

- Suffolk Constabulary, Police Headquarters, Martlesham Heath, Ipswich, IP5 3QS. Tel 01473 613500
- Norfolk Constabulary, Operations and Communications Centre, Jubilee House, Falconers Close, Wymondham, Norfolk, NR18 0WW.

## Appendix A – Information Asset – 'How to Comply' Checklist

This short checklist will help in assessing if the information asset(s) complies with the Data Protection Act 2018 if personal information is processed. Please note – being able to 'tick' every question does not automatically guarantee compliance. Please contact the Compliance Officer for advice as required:

| REQUIREMENT | YES |
|---|---|
| Is a list kept of who is able to access the asset(s) and at what level, i.e. administrator, editor, reader and is access to personal information limited only to those with a strict need to know? | |
| How is personal data collected and for what purpose? I.e. forms, direct data input (collection) and staff administration, policing and/ or ancillary support (purpose). | |
| Is consent required from those people whose information is retained and are they likely to understand what it will be used for? Is the information retained for any other lawful purpose? | |
| Is the personal information accurate and up to date? | |
| Are there processes in place to check the quality of data input? Are there spot checks/ cross-reference processes to help ensure accuracy of personal information? | |
| Is there clear guidance and rules on what information needs to be kept, and for how long and is information deleted/ destroyed as soon as there is no requirement to retain? | |
| Are the team/ department aware of the correct disposal requirements? | |
| Is adherence to these policies regularly checked? | |
| Is there robust security and protective measures in place including an assessment of the physical security of the asset? | |
| Is there an established auditing process to ensure compliance with the rules of operation for the asset? | |
| If personal information is requested, are staff clear when the Act or other appropriate sharing agreements allow disclosure to take place? | |
| Are staff trained in their duties and responsibilities under the Act and are they put in practice? | |
| How will the above be reviewed to ensure the asset is fit for purpose and processes kept up to date? | |

## Appendix B – Information Asset Checklist

Recording the detail below will help the IAO in recognising the current status of the asset and how it is utilised. Information Assets and any changes to the status of the asset must be notified to the Compliance Officer in order to ensure that the Information Asset Register is accurate and up to date.

| | |
| --- | --- |
| Description | Brief description of what the asset is.<br>More detail on what the components of the asset are.<br>Location of the asset. |
| Status | Is the asset being actively updated?<br>Has the asset been archived/ closed? |
| Date | Creation date<br>Date closed<br>Last date the asset was reviewed or updated |
| Purpose | What part(s) of the organisations does the asset support? |
| Value | What is the value to the organisations?<br>What would be the cost of replacing the information? |
| Use | How is the information found?<br>What do users need to be able to do with the information?<br>What needs to be understood about the information? |
| Risk | What are the risks to the asset?<br>What are the risks to the organisation from the asset? (i.e. from its loss, corruption of inappropriate access) |