Appendix 1

IMS2
Information
Management Strategy
2015 – 2020

"The PDNPA will hold and use high quality information in a secure, consistent and structured way to allow the maximum benefit to be realised from this asset. This information will be easily shared within the organisation and publically with customers and partners where appropriate."

Version	Status	Date	Amendment History
1.1	Draft	19 September 2014	Created by Jeff Winston
1.2	Draft	25 February 2015	Created by Darren Butler
1.3	Draft	09 April 2015	Created by Darren Butler
1.4	Draft	01 May 2015	Created by Darren Butler
1.5	Review	28 May 2015	Created by Darren Butler
1.5	Pre ARP	23 June 2015	Created by Darren Butler

Distribution:

Copy No.	Name	Role	Organisation
1.1	Darren Butler, David Higley, David McMahon, Lee Passarelli, Michele Sarginson, Tom Wiseman, Martin Wootton	ICT team	Peak District NPA
1.1	Mary Bagley, Maureen Eastgate, Ruth Marchington, Brian Taylor	Information Management steering group	Peak District NPA
1.3	Mary Bagley, Maureen Eastgate, Ruth Marchington, Brian Taylor	Information Management steering group	Peak District NPA
1.4	Mary Bagley, Maureen Eastgate, Ruth Marchington, Brian Taylor, Penny Aitken	Information Management steering group	Peak District NPA
1.5	SMT	SMT	Peak District NPA
1.6	ARP	ARP	Peak District NPA

1. Table of Contents

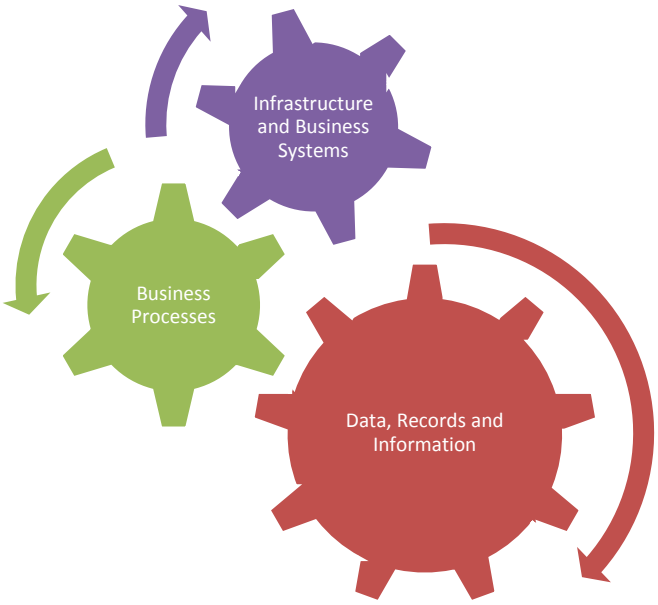
2. Introduction

This section will define information management and an information management strategy as well as describing the outcomes of the previous strategy.

2.1 Definition and Aim

Information Management is a broad term that encompasses the techniques an organisation adopts for the creation, use, processing/manipulation, publication and destruction of information. This includes the systems and processes as well as the data and information itself and aims to increase the value of information as an asset (through improving the decisions an organisation makes and/or improving the services it offers to its customers etc.)

An information management strategy (IMS) provides a corporate level vision, plan and discipline for how an organisation can make the best use of its information to increase productivity, responsiveness, quality, security and service offering whilst reducing risk, latency and duplication. An information management strategy must take into account the organisations data, processes and systems, and so is not a strategy for IT teams alone, but has an impact and dependency for all parts of the organisation.



This diagram illustrates that a combination of elements is required to improve the value of information as an asset, and that no single item (business or IT systems, processes or data) can deliver in isolation.

2.2 Background and Lessons Learnt

IMS1 (2008 – 2013) moved the organisations information management forward in a number of areas:

- The organisations infrastructure was improved to provide increased stability, security and resilience as well as data backup and disaster recovery provisions. This gave the organisation a fundamental foundation from which to build its capabilities whilst reducing its risks.

- Business processes were reviewed in some areas, and re-engineered together with new business systems to tackle issues with information storage, availability and efficiency in processes (specifically development control and pre-application advice utilising document management and PAM/DAM). This successfully tested the principle for storing information once, electronically, but making that information available from that single source to all areas that require it (both within the organisation and externally).

- The organisations spatial data started to be cleansed and migrated to a single consistent source (moving away from sporadic, duplicated files stored in multiple locations with limited control of versions or accuracy, and limited ability to share that information across the organisation)

Although these successes need to be recognised and continued, it is also important to learn from the challenges met during IMS1, which include:

- A greater need for governance at a corporate level to ensure that new processes, systems or activities are implemented in a way that compliments the organisations existing work and information and does not create separate 'pots' of data existing in silos.

- A need for an improved justification processes for new endeavours to prevent the organisation being distracted by activities that do not yield an adequate return for the organisation and/or its customers and divert resources from agreed priorities.

- A need to improve the utilisation of existing processes and/or systems to prevent areas of the business 'reinventing the wheel' when performing activities similar in nature to activities undertaken in other areas of the organisation.

In summary IMS1 provided a stable foundation, and tested the principles on a practical level. IMS2 now needs to build on that foundation to deliver the vision in a much more holistic way.

To supplement this introduction, please see appendix 1 for an overview of the organisations data needs both historically and at the present. This strategy aims to meet the current and predicted data needs for the organisation and its customers.

3. Vision for Information Management

"The PDNPA will hold and use high quality information in a secure, consistent and structured way to allow the maximum benefit to be realised from this asset. This information will be easily shared within the organisation and publically with customers and partners where appropriate."

3.1 Information Management Principles and Deliverables

Using the format:

1. *Principle*
    - *Deliverable*
    - *Deliverable*

This section aims to provide fundamental guidelines to align how information is managed to support the vision statement and provide an overview of the deliverables this will provide for the organisation. In approving this strategy these principles will underpin the way we work across the organisation in the future.

1. Information will be recognised as an asset and managed to a quality that meets business and customer needs. Includes assigning custodian ownership of datasets to provide accountability and ensure information is managed appropriately (Information Asset Owners (IAOs)).

    - Introducing management standards for information, including creation of Metadata about the information will allow a greater use of technology to increase the efficient storage of that information as well as increase opportunities for re-use of information (and the business systems used to manage that information) across the organisation.

    - Information that is spread across paper records or poorly organised electronic formats could be missed when required, either for internal business needs or for customer and/or legislative needs (i.e. missing the publication of information as part of an FOI request). IAOs accountable for the consistent management of information would reduce the likelihood of this risk.

    - Increasing the quality of information will reduce the risk of making poor decisions and determinations based on that information (i.e. increasing the quality of information regarding a particular site will influence any planning decision at that site).

2. Information will be stored electronically in consistent formats where possible (i.e. stored and managed to consistent standards)

    - Information held electronically can be included in appropriate backup and disaster recovery provisions. Information held only in paper format is at risk of being permanently lost (i.e. in fire or flood etc.)

- Consistent methods for accessing information will reduce the training overhead for staff and allow all areas of the business to interact with all appropriate business information on a level platform.
- Use of consistent applications and increased governance will reduce the risk of Underutilisation of business systems or additional expenses incurred due to procurement/development of similar business systems by different areas of the organisation.

3. Public information will be published unless there is an overriding reason not to.

    - Customer Self-Service capabilities will be improved making the publishing of more information online possible. This will reduce the administrative overhead in managing customer requests for information and in managing the publically available information itself.

    - Appropriately managed information will allow that information to be accessible within the organisation as well as publically (where appropriate) without additional effort to publish copies of data (i.e. removing the current approach to holding an internal version of data and a separate public copy of that data creating 2 duplicate datasets that require management over time).

4. Information will not be duplicated, but will be stored once and made available to all appropriate areas. This includes only holding information that the PDNPA is best placed to hold (i.e. not duplicating information managed/stored by other organisations).

    - Removing or reducing data duplication will reduce the cost of storage of that information and reduce the ‘clutter’ of information within the organisation.

    - Appropriate signposting to third party data will reduce the amount of information that this organisation holds as well as removing the administrative overheads in ensuring our copy of third party data is kept up to date.

5. Information will be appropriately secured and backed up (i.e. rights to create, view, edit or distribute information to be controlled), though information will be available to all unless there are overriding reasons to restrict access (Data will be owned by the organisation and not by individual teams).

    - Appropriate backup and disaster recovery provisions will prevent the organisation permanently losing information, and will reduce the temporary loss of access to information to a minimum.

    - Raising data ownership to a corporate level and allowing access to all data across the authority (unless there is an overriding reason not to – such as restricted access to personal HR data for example) will remove ‘data silos’ and allow teams to make better decisions as they will have an awareness of the existence of data that may be relevant to their activities.

- Data managed and stored in consistent methods are easier to secure appropriately to prevent data breaches or loss of sensitive and/or personal data. Auditability of this data and access to it is also made possible.

6. Only required information will be stored and information will be appropriately disposed of when its use is complete.

    - Disposing of information at the end of its use will reduce the cost of storage of that information and reduce the ‘clutter’ of information within the organisation.

    - Disposal of sensitive or personal information at the end of its use will form part of the organisations actions to remain compliant with legislation (such as the data protection act).

More detail is provided to describe these principles in appendix 2.

4. IMS2 Delivery

The delivery of this strategy will be achieved in many different ways, but at the most fundamental level it will be achieved by taking the vision and principles into account in all projects as well as 'business as usual' tasks. This needn't be onerous and simply means that when there are many ways of completing a task, that the principles above are taken into account when deciding how to proceed.

The sub-sections below provide the key messages for how this strategy can be delivered, though these are still deliberately kept at a high level to allow this strategy to be applied at a corporate level and to remain relevant for 5 years. Specific projects will involve as many or as few of the sub-sections below as are appropriate to that project. Further detail supporting these key messages can be found in the relevant appendices (referenced in each sub-section).

Following the acceptance of this strategy by management team, a more detailed action plan will need to be developed for each of the threads below, appropriately prioritised into service plans over the period of this strategy.

4.1 Governance

The information management steering group (IMSG) has been set up, with representation from each of the directorates within the authority as a governance body for information management.

This level of governance is required to ensure that projects are:

- Appropriately prioritised against other projects, particularly when there are resource conflicts between projects.
- In-line with wider strategies, primarily IMS2 and the corporate strategy along with supporting strategies (i.e. the asset management plan and the giving strategy).
- Appropriate, justified and sustainable after delivery

In addition, this level of governance should provide a layer of sanity checking to ensure one area of the business does not procure services, products or systems that conflict or overlap with services, products and/or systems in use elsewhere in the organisation.

As the IMSG matures, it will need to define criteria to determine the level of project that should be considered by the group.

4.2 Data Management

There is still a broad mixture for how data is managed across the organisation, complicated further by the different types and nature of the data that the organisation manages. The main groups of data are described below, but it should be kept in mind that within any area of the business and for any specific task or activity, many of the groups of data are used together to gather the required information from all of the data available.

There is no 'one size fits all' for managing the broad and varied data created and used across the organisation and so the delivery aims below should be strived for with an understanding that exceptions may and will exist in some cases.

4.2.1 Spatial Data

The corporate Geographic Information System (GIS), called Earthlight, should be used to store all spatial data. In the majority of cases (circa 90%) Earthlight is also the appropriate tool for the consumption, analysis and manipulation of spatial data, although there are cases whereby additional functionality is required for more detailed or complex analysis. In these cases MapInfo should still be used to perform the specific task requiring the additional functionality, but the underlying data should remain managed through Earthlight.

Each spatial dataset owned by the organisation should also be described appropriately using metadata. Again this is to be managed through Earthlight and will form a part of the organisations data register as well as forming part of the organisations obligations under the Inspire directive.

Please see appendix 3 for further information and reasoning behind this approach to spatial data management.

4.2.2 Data in Business Systems

Utilisation of existing business systems is to be increased to obtain a higher value for money from these systems. Also, existing business systems are to be rationalised to ensure the organisation is not operating multiple systems that cover the same or similar functionality. The development and/or procurement of further business systems is to be governed by the IMSG (supported by appropriate business cases) to ensure that an appropriate return on investment will be gained from any business system and to ensure that different areas of the business do not operate new business systems that conflict with or duplicate existing business systems.

The Hub (a web based business system developed by the PDNPA) is to grow to include further data from business systems as well as spatial data managed by Earthlight. This application will provide a single consistent location, or 'portal' for staff and customers (where appropriate using the public side of the Hub) to view the organisations data in a structured and controlled way, from the range of different sources. The business systems themselves (or Earthlight in the case of spatial data) will remain the correct location to alter or manipulate data, but the Hub will be a tool for viewing and consuming that data from a range of source systems across the organisation.

Please see appendix 4 for further information and reasoning behind this approach to business system data management.

4.2.3 Documents

Documents will be stored and managed in the document management system (DMS), utilising a range of tools to complete this:

- The Hub (currently possible to view and search for documents – further development to follow during 2015 to allow document metadata and document versions to be managed as well as documents to be deleted and/or replaced).

- Polled folders, the batch scanners and wide angle scanner – allows documentation to be uploaded directly to the document management system and appropriately categorised and linked to the relevant business data (i.e. a document is uploaded and linked to the specific conservation area record that the document relates to).

- The DMS front end – to be released for wider business use following a security update during 2015, this application will allow granular management of documentation including deleting and workflow management.

- Plugins for Microsoft office – this will allow documents stored in the DMS to be accessed directly from MS office products (such as word or excel) so that document content and metadata can be created, manipulated or updated directly.

The business data that the documentation relates to will need to be available within the Hub prior to any documentation being migrated into the DMS (for example this may involve the cleansing and migration of spatial data into Earthlight before the documents that relate to that data can be stored in the DMS).

Please see appendix 5 for further information and reasoning behind this approach to document management.

4.3 Information Asset Owners (IAO's)

The role of Information Asset Owner (IAO) will be assigned as part of existing roles throughout the organisation. These roles will be assigned to individuals to cover specific team or department levels as appropriate to provide a point of accountability and custodianship for the quality of the business data managed by that team/department.

The IAOs will be responsible for ensuring that data is maintained to required standards, stored and managed in accordance with this strategy and that the metadata is complete and accurate for each data set within their specific area. (for clarity, the IAO's will be responsible for ensuring the quality of the data and metadata maintained, not necessarily for managing the data and/or metadata themselves).

Once the IAO's are in place, the head of information management will also take on the role of Senior Information Risk Owner (SIRO) as recommended by the ICO and during the 2014 information management external audit.

Please see appendix 6 for further information and reasoning behind the use of information asset owners.

4.4 Infrastructure and Business Systems

A solid foundation upon which the organisations business systems operate, providing access to required systems and data to staff and customers as appropriate, managed by a combination of an appropriately skilled core in-house team and 3rd party support.

During 2015 and 2016 the organisations core infrastructure (the servers, network and storage equipment) are up for renewal. The preferred option is to move from a model of 5/6 yearly replacement of equipment purchased and hosted at Aldern House to a service model whereby the infrastructure is hosted and partly managed by a 3rd party. This option will provide scalability to grow or adjust the infrastructure as the organisations use of business systems matures, and as the organisations focus and functions change over the time period for this strategy. This option will also fill a skills and capacity gap within the in-house IT team for infrastructure management reducing the risks of system failures and issues. Specifically this will include enhanced management of firmware, software patching as well as management of key components such as the virtualisation software and application delivery software (such as Citrix).

Please see the related documents section below for a link to the business case and financial forecast for the organisations IT infrastructure replacement programme for more detail.

4.5 Skills and Training

Staff will need to have the appropriate skills to use the equipment, business systems, processes and data as appropriate for their role. The information management service will be responsible for training staff on in-house developed applications (such as the Hub), whereas training for standard off the shelf applications (such as MS Office or M3 etc.) will be managed by individuals and their line managers. Training on applications should be coordinated across the authority as much as possible to receive economy of scale savings for any training provided. Other training resources (such as Lynda.com) will also be promoted more to encourage a greater individual responsibility for maintaining skills and for self-led training.

4.6 Ways of Working

Data used by individual teams can no longer be considered in isolation of the rest of the organisation or the rest of the organisations data. Changes will need to be made in most areas of the organisation for how they store, manage, maintain and use their data (As per the IMS2 Delivery section above) to remove the current silos of data that exist within the organisation. This change will need to be managed in a way that is feasible and sustainable for each area of the organisation in turn to minimise the impact on service delivery during the time of change, but will need to be given enough priority so that these changes do take place. From that point consistency and discipline will be required to continue to manage data in a corporate way, and not revert back to teams keeping local ‘pots’ of data in their folder structures. IAOs will help to maintain this control.

Local departments or teams will maintain control over the management of data for their area, but the data must be considered as a corporate asset rather than a team or department resource alone.

5. Risks and Dependencies

This section aims to highlight the risks and dependencies within the organisation that will need to be addressed as part of the implementation. As an overarching strategy, these deliverables and dependencies will be kept at a high level. The justification and planning process for projects and specific items of work (for example a recently proposed data cleansing and migration project for ecology spatial data) will need to incorporate detailed deliverables and dependencies in line with this strategy and will need to mitigate the risks identified.

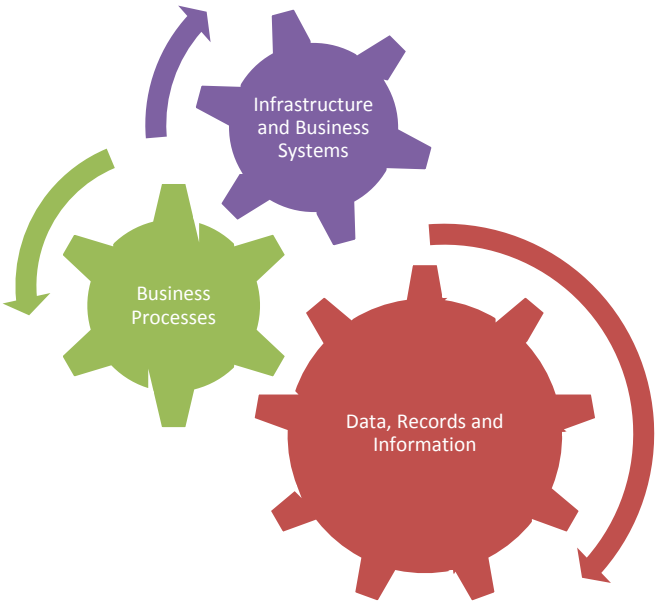
5.1 Risks for implementing IMS2

As with any area of work, changing the way in which the organisation manages its information does increase some risks (as well as reducing or mitigating other risks). This section aims to provide a high level view of any risks that would be created or increased by implementing this strategy, but again any specific items of work proposed would need to identify in detail the specific risks related to that piece of work.

Risk Description	Potential Impact	Mitigating Action
Increasing self-serve capabilities and publishing more information may allow customers to bypass an 'expert advice' process Likelihood and frequency are intangible as this risk is largely anecdotal.	Undesirable activities may take place for which the PDNPA has not had an opportunity to influence. For example, if TPO data is published, then a customer may undertake work on a tree (as it does not appear to be protected) that the PDNPA would have preferred to advise or prevent.	Each data set that the organisation holds must be managed based on its own merits, and only published where appropriate (including accepting any risks that may be present). The ability of the organisation to continue to provide an advice level service for the information that it holds will also need to be taken into account in light of the financial challenges the organisation faces.
Increased risk of providing misinformation internally and for customers if quality, accuracy and timeliness of data is not maintained	Poor decision making by the organisation (when consulting or advising for example) or misdirection for customers	Information asset owners provide administrative ownership and clear boundaries of responsibility for the organisations information and data sets. Implementation of this strategy provides clear summaries for the organisations data making it easier to highlight and plan maintenance of data sets.

5.2 Dependencies

As mentioned in the introduction, good information management practices cannot be delivered by one area alone and instead requires three main areas in unison:



A business system alone cannot provide all of the benefits and deliverables of good information management practices as there is a reliance upon the business processes to control how the business system is used, and the quality of data to ensure the outputs of the processes and the information gleamed from the business system is fit for purpose. Likewise, simply having high quality data in isolation of business systems and processes will limit the benefits as the business system provides the functionality to manage, manipulate and consume that data in more meaningful ways, increasing its value in combination with sound business processes to ensure the data remains high quality, accurate and fit for purpose as well as used in the most efficient way.

6. Related Documentation

The following documentation relate to this strategy, though some items are confidential in which case only management team and the IMSG will be able to open them:

- IT Infrastructure Refresh Business Case
- IT Infrastructure Refresh Financial Implications (Confidential)
- PDNPA Sites - Connectivity

7. Appendix 1 – Understanding the data needs

Historically the organisation has been largely ‘site focused’, deriving most business activities from areas of land across the national park. This is reflected in the organisations data, whereby a high proportion also relates to sites. This may be in the form of:

- National or international designations such as Sites of Special Scientific Interest (SSSI), Countryside Rights of Way (CROW) or Scheduled Monuments etc.
- Landholding or land ownership such as Coal Authority land, natural England owned land or PDNPA property and trails etc.
- Localised designations or areas of interest such as archaeological sites, planning matters or event routes/locations etc.

Note: the data sets above list only a tiny amount of the data that the organisation holds or uses and are listed as examples only.

Although the organisation holds a significant amount of data, files and records for a range of subjects, in nearly all circumstances that data at least relates to an area of land. This data would generally have been stored in a range of paper filing methods across the organisation and although storing information in paper format has greatly reduced (but has not yet completely stopped) it does mean that there is a legacy of large volumes of (still relevant) information that is only held in paper format.

In recent years the organisation has recognised the risk in storing information in this way (i.e. lose the paper record and you lose the information permanently) as well as the difficulties for information provision and usage that this causes (i.e. the time spent searching for the relevant paper record, or the inability to publish paper information to customers in an efficient way). This realisation prompted a shift to storing information electronically, though initially this was implemented in an ad-hoc way (for example files are stored in differing folder structures and ‘buried’ in multiple folder levels with little or no consistency for structures between teams and services). This shift did help to reduce the risk for permanent loss of information, but did little to help the efficient use of that information across the organisation or to make relevant information available publically (i.e. the information was still held in silos where one part of the organisation would be un-aware of what information was held by another part of the organisation, and therefore unaware of whether that information is useful to their activities or not).

Today, the organisation still has a large focus on sites, but is also shifting to include a greater focus on customers as well. Also, through the implementation of IMS1, new tools are allowing the organisation to store its information, or at least pointers to that information, in a way that makes it available to the rest of the organisation in a consistent and controlled way (i.e. the use of Earthlight for spatial data and PAM/DAM and the HUB as a ‘window’ to view information from multiple sources). At the very least this allows knowledge of the existence the information the authority holds to be known to wider audiences than simply the team that created the information, but where possible and appropriate also allows access to that information without having to ‘proxy’ requests through other teams. In addition, there is a growing desire from the public, and mandate on local government authorities to increase transparency, and publish much more information than would have been published historically. This trend is only set to increase, meaning a greater demand on the organisation to service information requests from the public if that information is not readily available in a ‘self-serve’ capacity.

IMS2 will seek to continue this maturing approach to information management, and support the growing need to relate information to customers as well as sites, increase the knowledge of, and ease of access to information within the authority, as well as increase the capability for customers to self-serve to retrieve appropriate information.

Appendix 2 – Information Management Principles Detail

Principle 1 describes how information will be recognised as an asset within the organisation, in a similar way to finance, physical assets (property) and/or staff. As an asset, information will be managed in a way that will allow the organisation to hold it in a secure and efficient way, but also make the most use of that asset to meet the aims of the organisation. This will include the assigning of appropriate information asset owners (IAOs) as recommended by the information commissioner's office (ICO) for public bodies. These IAOs will be responsible for ensuring that information is managed to suitable standards to ensure it is fit for purpose and available to all appropriate parties and that the information is not duplicated, remains up to date and meets required quality standards. These standards will include maintaining information asset registers with appropriate metadata to describe the information being held (for use within the organisation and publically where appropriate).

Principle 2 continues the theme from IMS1 whereby a paper record will no longer be the master copy of any piece of information. The organisation has a legacy of large volumes of paper files with very limited resources available to change this. However, for any new information created, or if any information is updated it should be stored electronically in as consistent a method as possible (dependent on the type of data in hand). This means that wherever possible systems and standards will be re-used to reduce the number of disparate locations that information is stored in. Greater use of a document management system should be used to reduce the amount of information stored in windows folders increasing the control, access and search ability of these records. Corporate applications such as the HUB should be utilised to publish information (or at least publish the description of that information) across the authority and publically where appropriate. For example, it may not be appropriate to publish the details (reports and findings etc.) of a particular land survey, but the existence of that survey should be published. Using a single application such as the HUB to publish that information (either within the authority or publically) regardless of the actual source of that information provides a consistent application for staff to use regardless of the type of information.

Principle 3 is derived from a UK central government principle for information management, and also supports the aims for government organisations to become more transparent. In practice, this principle needs to be applied in a way that:

a) Reduces the administrative overhead for publishing information by allowing the information to be stored once and made available publically from that location where appropriate. This will mean a shift in some areas where by information is stored and managed in one location, and then a copy is made and stored in another location (such as a pdf for our website) to be published.

b) Allows the public to access that information in a 'self-serve' capacity to reduce the administrative overhead in preparing and supplying information following direct contact from customers requesting information.

Principle 4 describes a behaviour that will increase accuracy of information as well as reduce the cost for the storage of that information. For example, currently if a report is required by 3 teams within the authority, then there are examples whereby that report will be copied three times and stored individually by each of the teams. This both increases the cost for that storage (as the report is effectively taking up 3 times the space) and prevents appropriate version control (as not all copies may get updated if a change is required, potentially leaving one team working from an old version). This principle states that a piece of information will be stored once, but made available to all interested parties through appropriate means (such as the HUB or M3 for example).

Principle 5 states that all information will be made available across the authority unless there is an overriding reason not to (such as particular licence constraints or data protection matters etc.). At the very least, descriptions of the information will be made available to increase the wider knowledge of the information that the organisation holds. Appropriate security will be applied (through business systems or user accounts etc.) to control access to read, create, update and dispose of information. Data stored electronically will be appropriately backed up and covered by appropriate disaster recovery provisions to reduce the risk of permanent loss of information.

Principle 6 aims to control the organisations remit for information and ensure that the costs for storing information are only incurred where required and for as long as required. Only information that the PDNPA is best placed to store and manage should be held. The PDNPA will signpost to information that other organisations are best placed to store and manage rather than holding copies of information held elsewhere. In addition (and particularly pertinent for personal information under the DPA) the PDNPA will dispose of information when it no longer has a use for that information.

8. Appendix 3 – Spatial Data Management

All spatial data managed by the organisation should be managed using the corporate GIS tool – Earthlight. This tool abstracts the complication of the physical storage of data as it is driven by a database backend. In contrast, tools such as MapInfo force data to be stored in flat files that had to be managed by the individual teams using the application (it is acknowledged that MapInfo can link to databases, but in practice this is unreliable and has a performance cost making MapInfo very slow to use in this way, particularly with large data sets). This has led to a state whereby there are thousands of tab files stored in differing folders and folder structures that overtime have become unfamiliar, even to the teams that created them. There are many copies of data with limited or no version control, leading to situations now where it is simply not known which version of a data set is the most recent or accurate.

At the worst point (during 2012), the PDNPA held over 56,000 MapInfo datasets including many duplications. This number is too large to manage and too large to use in business as usual activities effectively.

With the use of Earthlight, stricter rules can be enforced to control spatial data to ensure that any dataset only exists once, and that the specific fields within a dataset have appropriate validation rules (i.e. to ensure a numeric field only has numeric values, or that a date entered is actually a valid date etc.). Migration to Earthlight has already started to reduce the number of spatial datasets significantly, but this work must be continued as part of the implantation of this strategy.

Tools such as MapInfo are still useful in some circumstances, for example if complex spatial analysis is required which is either above and beyond the functionality within Earthlight, or is easier/quicker to achieve in MapInfo. This should not be discouraged as removing MapInfo altogether would be ‘throwing the baby out with the bath water’. To achieve this Earthlight (and its backend database) can be used to setup controlled replication of required datasets into MapInfo formats to allow it to be used within MapInfo. These replicated datasets should be removed when their use is no longer required and should not be updated directly (i.e. they are read only to maintain the version control for the master dataset used in Earthlight). There are cases whereby MapInfo can access the same datasets in the backend database as used by Earthlight, though these cases are infrequent due to performance issues for MapInfo operating in this way.

Finally, managing spatial data in this way allows metadata to be stored for each spatial dataset. This not only helps the organisation meet its obligations under the INSPIRE directive, but will also allow the organisation to publish (internally and externally – as appropriate) information about the spatial data that the organisation holds. Increasing awareness of the organisations information in this way will both prevent situations whereby one area of the organisation duplicates effort by managing a data set that already exists in another area of the organisation, as well as allowing areas of the business to decide which data needs to be taken into account for specific activities instead of limiting them only to the data that they are aware of or hold themselves.

The migration and cleansing of spatial data from MapInfo into Earthlight has been taking place over the last 18months (at time of writing) but has not yet included all spatial data across the organisation. This migration will need to continue, but varies in magnitude based on the complexity and quality of the existing data. This migration will need to continue in a priority order taking into account the capacity within the teams that own the data in question.

9. Appendix 4 – Business System Data Management

A large proportion of business data is held in various business systems, such as the M3 planning system, exchequer finance system, TF Facility asset management system etc. the authority has a mixture of off the shelf (OTS) business systems as well as custom built business systems (either developed in house or by 3rd parties). Business systems in general allow both the data to be stored in a structured way (level and quality of structure depends on the particular business system) as well as providing a level of workflow management to aid in the business activities that the data in the business system is related to.

Business systems provide a range of benefits including:

- Workflow management (providing efficiency savings for completing tasks)
- Security control (i.e. ensuring only the correct people can view, update and/or remove information)
- Audit control (often meeting compliance regulations)
- Automated or part automated processing (providing efficiency savings for completing tasks)
- Validation and quality control (ensuring required data is not missed and that only valid values are entered etc.)

Due to this, the use of business systems should not be discouraged, however, use should be strictly controlled. Business systems epitomise the constraint that there is no 'one size fits all'. This simply means that there is no single business system that can support all of the different types of activity that the organisation undertakes and so a mixture of different business systems for different purposes will always be required.

Due to this, it is inevitable that separate pots of business data will exist in separate systems, though some level of integration should be implemented. Currently the organisation uses the HUB to provide this integration. This application allows data from multiple different sources (including different business systems) to be viewed in a single location, though the original source of that data remains the location whereby that data is created, manipulated or disposed. This allows a single consistent application to be used in cases whereby data only needs to be consumed.

The use of multiple different business systems is also where the control should be greatest as there is opportunity for some re-use of business systems, and so new systems should not be procured or developed in every use case. Instead decisions involving business systems need to take into account:

- Whether the organisation has or uses an existing business system that could meet the needs (i.e. don't have 3 teams managing customer enquiries in 3 different ways utilising 3 different systems). This may involve some compromise of the process or service and/or some enhancement of the existing system.
- Whether the business system proposed integrates with any existing systems or can be used with the HUB.

Any business case for new business systems should take these points into account, and should be filtered by the IMSG as part of the governance and control of corporate level business systems.

10. Appendix 5 – Document Management

The organisation holds documentation that relates to a range of different subjects, which are held in a range of formats (including different electronic formats such as PDF, MS office documents etc. as well as in paper format). The documentation is also held in a range of different structures and locations (physical locations for paper records, and different folders and folder structures for electronic documents, with some areas of the organisation utilising the document management system). There is also some duplication of documentation in cases whereby it is required by more than one part of the organisation (i.e. both business areas will hold a copy of the same document for their own purposes, and this sometimes includes a mixture of paper and electronic formats).

As stated in the principles, the master copy of a document should no longer be a paper document. Unfortunately, however, an exception will need to be made for the large quantity of existing paper records as there is little resource available to cleanse and scan this content (though occasional projects do take place that tackle pockets of paper records as and when they are possible). Due to this the organisation will have to accept that some documents will continue to solely exist as paper records, but any new or updated documents should be stored electronically only. This does not remove the use of paper records, as they do have a use, but simply states that the master copy of a document will only be held electronically (i.e. a printout may be appropriate in order to complete a specific activity or for reference, but the paper copy should be disposed of at the end of that activity).

Holding a document electronically is not enough on its own to improve the management of the organisations documents. Further control over the storage of electronic documents is still needed to maximise the benefits of this. Currently some documentation is held in the document management system, whereas the majority of electronic documentation is held in inconsistent folder structures on the authorities main file server. Use of the document management system is the preferred method for document storage for the following reasons:

Benefit	Description
Data Storage	Documents in the document management system can have a level of automatic archiving applied whereby the documents would remain available, but those documents that have not been accessed in a period of time (perhaps 6 months) would be stored in a compressed state and on cheaper storage technology. When the document is next accessed it would be decompressed and returned to the primary storage array where it would remain until it was not accessed again for the designated time period. No quality would be lost in the document, though the first time the document was accessed from the archive location would take more time than usual to open due to the decompression taking place first. This could reduce the storage requirements for documents accessed infrequently by up to 90% (dependent upon the format and content of the document) reducing the storage capacity needed accordingly. The use of a cheaper storage array for the archived documents reduces the cost of this storage capacity further (please see the IT Infrastructure Refresh business case for full details)
Workflow Management	Where appropriate, the document management system can be used to apply automated workflows for documents both reducing the administrative overhead in managing those documents and potentially increasing the timeliness, accuracy and quality of documentation. These workflows could be as simple as automatic notification when a document reaches a designated review date or as comprehensive as full lifecycle management of a document as it moves through draft, QA, approval, go live, review and update/disposal (with the document being automatically passed to the relevant staff for each stage of the process).
Version Control	It is much easier to apply version control to documents in the document management system where required. The latest version of a document will be displayed by default, but the previous versions can be viewed easily whereas holding previous versions of documents in windows folder structures can clutter the view of documentation. Version control need only be applied where appropriate so that if a previous version of a document is not required once it has been superseded, then it can be disposed of.
Document meta data	Information about the document can be held as meta data to provide a greater description of the content and purpose of a document, as well as which subjects or other data sets that document relates to. This is possible with MS office documents stored in windows folders, though in practice it is not used due to the convoluted methods for populating and viewing meta data for files stored in that way. Meta data increases the information available about a document which in turn allows for greater decision making when deciding which documents are relevant for particular activities.
Search and navigation	The document management system allows documents to be searched and viewed easily, using either the content of a document (dependent upon the format and type of document) and/or the metadata of a document. This allows documents to be retrieved without having to navigate through multiple levels of folder structures (particularly pertinent when one area of the organisation wishes to view a document managed by another area of the organisation as the folder structures used may be unknown or unfamiliar making it difficult to find the required document or easy to miss relevant documents). Again there are alternative add on tools available that allow documents that are stored in windows folders to be searched, but these tools are limited if the meta data is not used as they can only use the document name and/or its content (again dependent upon format and type of the file) to perform the searches.

It is rare that a document exists in isolation of any other business data. In the majority of cases a document will be related to a specific subject, which exists as a quantum of data somewhere within the organisation. For example, a document may relate to a listed building, or to a particular survey that took place, or to a customer enquiry, or to a particular land designation etc. in these cases there will be a data record detailing the listed building, or the survey, or the enquiry or the land designation. For example there is a data set of listed buildings, and the document in question will relate to one of the records in that dataset (i.e. to a specific listed building). In these cases, the first step is to ensure the underlying datasets are managed appropriately (see the spatial data and/or business systems sections for details). This means that the records can be presented in the HUB for relevant staff to view. The documents can then either:

1. Be uploaded to the document management system with appropriate meta data linking the document to the relevant data record (i.e. the particular listed building record)

    - This is the preferred method as the documents can be viewed in the HUB directly and can be published outside of the organisation easily where appropriate.
    - This option gains the benefits listed in the table above.

2. Be stored on a file server in a structured way so that from the data record in the HUB a link is possible to allow staff to navigate directly to the location of the relevant documents.

    - This removes the need for staff to be familiar with specific folder structures used by the various teams in the authority.
    - This would limit the ability to publish documents as the file server is only accessible internally.

Again, it is important to reiterate that there is no ‘one size fits all’ solution for managing documents, and that documents should be grouped by subject matter to determine the best method for managing particular groups of documents. The management method above should be viewed as the preferred method, but in specific use cases there may be overriding reasons to manage particular documents in other ways. The number of different approaches however, should be kept to a minimum to provide consistency across the organisation.

11. Appendix 6 – Data Quality and Information Asset Owners

It is a strange concept that data can get ‘lost’ within an organisation, but over time this can, and in some cases, does happen. This is particularly pertinent for data that is used infrequently. Data can become buried in folder structures and forgotten about, particularly when staff changes take place between its usage periods, meaning that either activities take place without the knowledge that the ‘lost’ data could have provided, or the ‘lost’ data is recreated, costing time and effort as well as the cost of physically storing the same data more than once. Even if the data itself is not lost, its meaning can be if the data is poorly structured or if there is little or no information about the data available to describe it.

Information asset owners will provide points of responsibility throughout the organisation for maintaining data to a required standard. This will include maintaining metadata about the organisations data to a consistent standard. As well as this, information asset owners will provide the mechanism for a consistent approach to data storage across the organisation, allowing greater utilisation of business systems and increasing the value of the data the organisation holds.

Use of Information asset owners is also a recommendation from the Information Commissioners office (ICO) and a regular recommendation from the organisations auditors as a way of providing a level of accountability for the management of information as an asset across the whole organisation in a formal and controlled way.

IAOs will form part of the control mechanisms required by the Senior Information Risk Owner (SIRO) role which has a wider responsibility for managing the levels of risks associated with the varying types of data that the organisation holds and manages as well as the provisions in place to mitigate those risks. The full domain of the SIRO is out of scope of this strategy, but is mentioned here as there is a dependency upon the implementation of this strategy and upon the IAO’s for the SIRO to perform the required duties as recommended by the ICO.