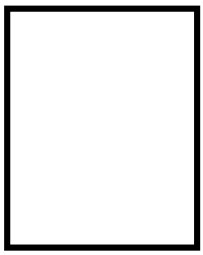


Dacorum Borough Council Corporate Information Assurance Protocol

Number:	**DBC000 IAP**	**Title:**	**Information Assurance Protocol**				
Owner:	**AD – Legal, Democratic & Regulatory**	**Rev**	**1.4**	**Date**	**2nd August 2012**	**Classification**	**UNRESTRICTED**

Contents

Introduction

This document forms part of the new 'Information Assurance' suite of policies, procedures and forms, authorised by CMT following an information security review and implementation plan.

This document is over-arching and encompasses the 'Information Assurance' spectrum namely; Information Security, Information Management and Compliance, Records and Document management and external and internal drivers for change and implementation.

This is a Corporate Information Protocol and includes associated ICT elements.

This reflects the fact that an Information Assurance Protocol cannot exist in isolation as the influences of ICT along with the way we manage information assurance and the changing requirements for the way in which an Authority provides services to the public are interdependent and need collective consideration in an overall Protocol document.

Scope of the Information Protocol

To be effective, an Information Protocol cannot focus purely on the ICT services within the Council, but must consider the drivers influencing the service from both internal and external sources. It must also reflect the fact that ICT services are just one part of the equation. This document focuses on four interrelated elements, each of which feeds into the overall Information Protocol. The four factors making up theProtocol are as follows:

- Internal Information Assurance Influences – these elements explain the way in which the information held by the authority should be organised and managed. There are many influences from internal sources that impact upon this process and which need to be fully considered by the Authority when managing existing information or developing new information systems.

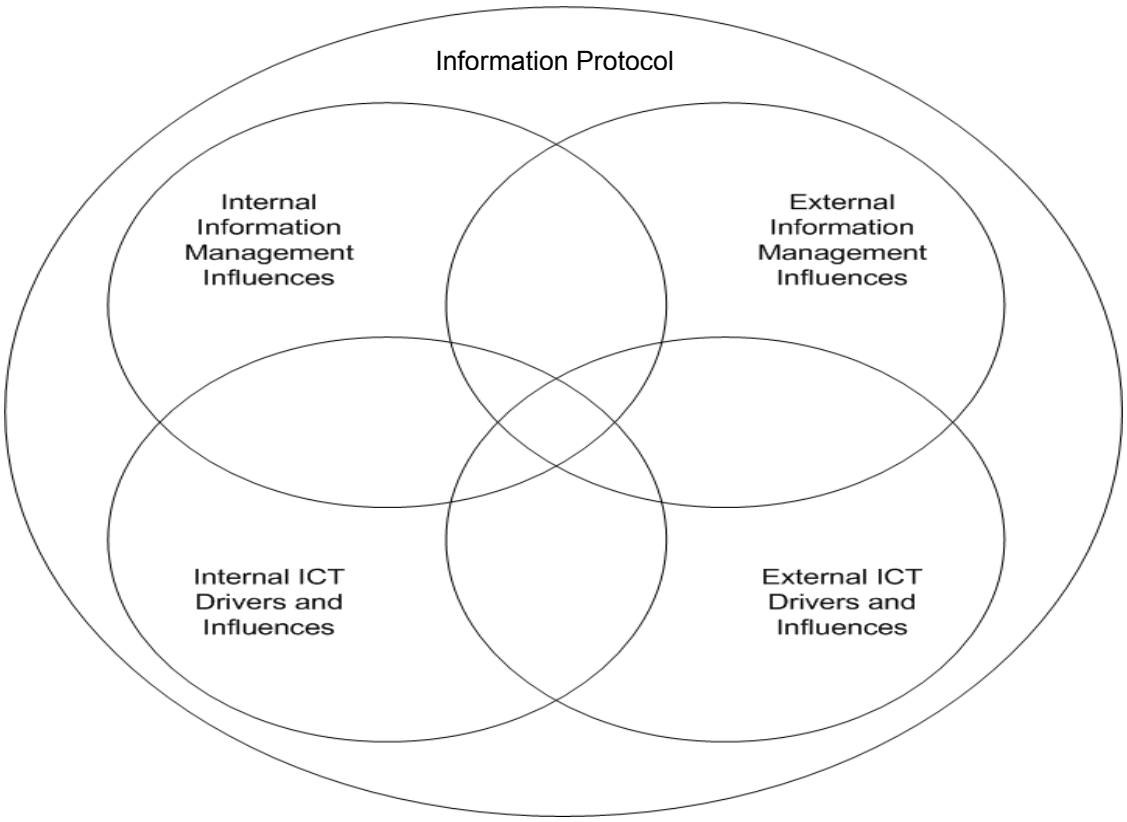
- External Information Assurance Influences – In addition to the internal decisions about how information should be managed, there are a number of external / legislative influences, which enforce the way information is handled.

- Internal ICT Drivers and Solutions – These are the technical aspects of the Protocol that enable the other aspects of the Information Protocol. These technical solutions have been identified to support the corporate priorities of the Authority, to facilitate the better use of information as identified in the Information Assurance requirements section and to help meet the shared, modernisation and localism drivers.

- External ICT Drivers and Solutions – As with the Information Assurance Influences, there are certain situations where the direction of the technology in use at the Council is determined by external factors. These external ICT drivers which need to be considered as part of the overall Protocol include (but not limited to) the Government Connect Programme (GSi / GCSx) and ICT Shared Services arrangement.

Structure of the Information Protocol

As has been discussed, this overall Protocol document consists of four separate elements, namely, the Internal and external Information Assurance elements and the internal and external ICT drivers and solutions. Despite each of these being separate sections, they are interrelated and impact upon each other.



Representation of Information Protocol

Each of the four elements included in the Protocol, have been constructed in a similar way. For each, there is an overview, a list of high level objectives and a summary of each of the elements that will be addressed to meet that part of the Protocol. This document does not provide a detailed analysis of each of the elements included at this stage, but identifies them as potential items for further investigation. It will be the responsibility of the individual project managers and the ICT team to take forward the process of assessing the suitability of these projects and subsequently planning the implementation to take the Authority forward.

It is important that the Information Protocol is a 'living document' and that progress against each of the elements is regularly monitored and reported.

Element A –'Information Assurance Influences'

Introduction

Information is a key business asset and the management of that information through its lifecycle from creation to archiving / deletion is critical to the delivery of public services. To deliver high quality customer focused services, Dacorum Borough Council must provide fast and convenient access to information relevant to user needs, both internal and external. That information must centre on the needs of the customer and not on what it is merely convenient to provide.
The key principles of Information Assurance are;

1. Confidentiality
2. Integrity
3. Availability
4. Accountability

Often known as the C.I.A.A square

Stakeholders Scope;

- The residents of Dacorum. Visitors to Dacorum
- Staff Members
- Councillors
- Partner organisations and business
- Charities

The area of Information Assurance examines the way in which we use information in order to assist our decision making and to help us be more efficient in the way in which we deal with the public. This element of the Protocol also defines the specific standards which enable us to use and manage our information effectively.

Objectives

The objectives of the Information Assurance element of the Information Protocol are as follows:

1. To establish and maintain principles and policies for managing information and security with a view to improving stakeholder access to information

2. To establish and maintain a framework for managing information to ensure effective and efficient use of time

3. To manage information compliance in accordance with statutory and legislative requirements

4. To create and adhere to policies, procedures and guidance to maximise opportunities for remote / home working, information sharing and partnership working, and ensure compliance in accordance with the Council's code of conduct.

There are a number of initiatives in place that impact upon the area of Information Assurance and that will assist in achieving the objectives detailed above. Many of these have partially been addressed, whereas others will need to be built into future work programmes. Descriptions of the specific areas needing to be addressed in the Information Assurance element of this Information Protocol are detailed below. These areas will need to be fully examined and evaluated as part of the project management process for implementing or developing them.

Internal Influences

1. Records Management, Disposal and Retention

The three most important and influential organisational drivers for reducing paper and digitising information are;

a) Public Service Quarter {PSQ} (est. 2016)
b) Civic Centre move (est. 2014)
c) Flexible working

There is a requirement to establish and document the requirements of each section for the periods of time documents should be kept before being disposed of. This is a particular problem because of the amount of paper that is currently produced and retained. Further Corporate implementation of Electronic Documents and Records Management EDRM will help alleviate the problem because of the increased amount of paper being converted to electronic form and the use of deletion dates pre-set on document types to automate the process.

The requirement for 'paperless' and digitisation is ever increasing, and the ability to have access to documents and records securely, with correct authorisation is paramount.

Having a dependency upon paper will impede flexible working. Staff working from home will not (or should not) generally have access to paper-based records.

The PSQ and Civic Centre move projects requires the council to significantly reduce its space requirements. Reducing both the use and storage of paper-based records is a way to achieve this objective. Given the timescales, it is suggested that unless the council starts very quickly to implement EDRMS, it will not be ready in time for the move out of the Civic Centre in 2014.

In particular, consideration will need to be given to:

- ***Information Auditing – resources need to be available to assess the paper records we have in the estate.***
- Reducing physical storage space (to support the office strategy)
- Increasing and improving electronic storage (to support and enhance search h capabilities e.g. reducing the burden and increasing the turnaround time for FOI or DPA requests)
- Storing information and data so that it can be accessed through hot-desking, and remote working arrangements

- The need for electronic collaboration, taking account of variable working practice and a reduction in co-location
- Improved personalisation of electronic workspace, so that people can work more effectively
- The length of time information and data must be stored for (to comply with statutory requirements that may extend for a considerable length of time).
- In line with a robust retention policy – the records management cycle of create, maintain, review, archive / destroy will be facilitated

Flexible working will increase significantly up to and beyond 2014. In order to accommodate the requirement to work at home or 'hot desk', the same level of security and access authorisation to information, must be applied in equivalency to the previous working environments.

Reduction in manual or 'paper' records is key to the requirement, in order to reduce the risk of breaches of either information security or Data Protection.

The Council's Flexible Working programme will introduce new working practices. These will be tailored to local working environments, but consideration will need to be given to how the service areas information assets are used and managed in order to support these changes.

Consideration will need to be given to the use of protective markers i.e. PROTECT, RESTRICTED in order to classify and authorise appropriate access. Protective markers are a mandatory requirement of the Government Connect Code of Connection (CoCo)

Specific Targets

- Information Audit – A Questionnaire to be sent to services in order to establish the 'baseline' view of paper within the DBC estate.
- Records Management Policy, Disposal Policy and Retention Policy, reviewed and updated to incorporate current guidelines, and best practice.
- Incorporate Home / Working strategy into revised policies.
- EDRMS Project Team established, Business Case and PID created with a view to Corporate roll-out.
- At least annual review of policy documents or critical updates when required
- Restricted marking for e-mails, review requirement for other documents.
- To enhance flexible working, by providing authorised and secure access to digitised information.
- To provide a security framework, through organisational, technical and physical means to which access to information is layered
- To provide compliance to relevant information and security legislation

2. Policy and Procedure

There are several policy and procedure documents in place to govern the use of ICT and Information Assets in Dacorum Borough Council. These documents have been written to offer guidance to staff on the most effective use of the facilities and to advise them on the rules they should follow in order to avoid any potential breeches of statutory requirements. The guidelines are made available to all staff via the Corporate Intranet and during the induction process. At the start of each day, all staff are required to confirm that they have read and understood the guidelines by clicking a confirmation button during their normal login process. It is important that the guidelines currently in place are reviewed, amended and added where necessary.

Specific Targets

- To review, refine and updateall ICT and Information Assurance related policies and procedures as and when required to ensure that Officers and Members make the best use of the ICT systems they have available to them, and to make staff aware of responsibilities they have to comply with legislative or locally determined best practice.

3. Software Licensing

It is important that the Authority maintains accurate records of the licensing arrangements in place across all departments and users. The keeping of such records ensures that the laws governing software piracy are not breached and that the Authority is receiving value for money by having the correct number of licensing for the required number of users. Reviews of the licenses in place should be conducted regularly to ensure that this is the case.

Specific Target

- To conduct an annual audit of software licenses and to compare the findings against a centrally held register.
- To maintain and update the software register in accordance with best practise

4. Information Security

ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). The standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

In addition to meeting the security standard, it is considered best practice to conduct regular penetration testing to ensure that an independent test is completed of the

vulnerabilities of the Authority's network. This test should be completed annually to ensure that new threats are protected against.

The main drivers for information security at the Council are;

- The Council's undertaking to the Information Commissioner
- Information Security Audit and follow up project plans
- Government Connect v4.1 Code of Connection Compliance
- PCIDSS Compliance (taking of payments and credit / debit card information)
- ISO 27001 Information Security Management System (adopt best practice)

Specific Targets

- To assess the requirements and adopt best practice for meeting the Security Standard ISO/IEC 27001:2005
- To implement, maintain and review the actions of any information security audits
- To implement the mandated actions in the Government Connect v4.1 Action Plan.
- To implement the actions in the Information Security Project Plan (derived from 2011 audit).
- To assess the requirements and adopt best practice for meeting the PCIDSS standard.
- To provide training and guidance on information security practice and legislation including (but not limited to); Information Security, Data Protection and Freedom of Information.

External Influences

1. Electronic Government Metadata Standards (E-GMS)

Metadata refers to the ways in which data is referenced, identified and retrieved. Standardisation of metadata throughout local and central government will considerably ease access to information and services by citizens and businesses. The metadata framework published in May 2001 provides a structure for standardising the tagging of information resources on web sites and elsewhere, with mechanisms to dynamically link related information resources and services. The Metadata Standard will define the elements, refinements and vocabularies and other encoding schemes to be used.

Specific Targets

- To ensure the use of metadata for all electronically published information within all areas of the organisation to ensure that data is referenced suitably, so providing easier access for other organisations and the public.

2. Data Protection Act 1998

As well as registering our need to process data with the Information Commissioner, there are 8 principles that must be followed in order to comply with the Data Protection Act 1998. The eight Principles state that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in line with your rights;
- secure;
- not transferred to countries without adequate protection

It is important that the Authority follows these principles and informs staff of their responsibilities. This has already been done via training, policy, procedures and guidance on the Intranet, but the Council will need to continue to ensure that the awareness still exists and that staff continue to comply with the Act.

In addition to the responsibilities on the Authority, the Data Protection Act provides the public with right to see the data held about them. All members of the public are entitled to see the information held by the Council unless the data falls under certain exemptions. Under the 1998 Act, this is the case for electronically held information and certain paper based records.

Specific Targets

- To continue to comply with the Data Protection Act 1998 and to react to any future changes in policy that the Act may require.
- Review notification entry prior to renewal each year
- To ensure that staff are aware of their responsibilities under the Act by conducting induction briefings and training for all Officers and Members.
- To insure that all requests for information (not subject to an exemption) are disclosed within the statutory working time limit.
- To provide useful specific Council guidance notes relevant to Council operating procedures and practices. Operating as a dynamic knowledge base of frequently asked requests.

3. Freedom of InformationAct 2000

The Freedom of Information Act 2000 has been in force since 1st January 2005.
The Act gives the general right of access to all types of "recorded" information held by public authorities (and those providing services for them), sets out exemptions from that right and places a number of obligations on public authorities.

Public authorities have two main responsibilities under the Act. They have to adopt and maintain a "Publication Scheme" and they have to deal with requests for information.

A Publication Scheme must set out the types of information the authority publishes, the form in which the information is published and details of any changes. The Scheme must be approved by the Information Commissioner who is also responsible for the enforcement of the Data Protection Act. Every Public Authority must publish information in accordance with its Publication Scheme and from time to time review its Publication Scheme.

In adopting or reviewing a Publication Scheme, a Public Authority must have regard to the public interest in allowing public access to information held by the authority and in the publication of reasons for decisions made by the authority.

The Council must ensure that responses to requests for information are performed in accordance with the Acts Section 45 Code of Practice, and in any event – in a timely manner – within 20 working days (if not subject to exemptions)

Specific Target

- To review the Council's Publication Scheme in accordance with the model guidelines placed on the Information Commissioners web-site.
- To ensure continued compliance with the Freedom of Information Act by maintaining necessary policy, procedures and guidance to deal with information access requests.
- To insure that all requests for information (not subject to an exemption) are disclosed within the statutory working time limit.
- To comply with the Freedom of Information Acts code of practices namely; Section 45 – Dealing with an information request and Section 46 – Codes of Practice on Records Management
- To provide training and updates to staff and members on the Freedom of Information Act 2000
- To create an F.A.Q and disclosure log – to alleviate the burden on the back office, and provide proactive / pre-emptive information in relation to requests.

4. Reuse of Public Sector Information

The Re-use of public sector information directive has been in force since 1st July 2005.

In practice, this means that when the Council releases information to the public which has been requested under access to information legislation such as the Freedom of Information Act 2000, the member of the public/the applicant may ask if they can re-use the information, perhaps for commercial purposes, in a way which, without permission, might breach the Council copyright.

An example could be, that Council has an internal procedure note which is sought under the Freedom of Information Regulations and thereafter the person who requested it may wish to reproduce that procedure if they think it represents Best Practice.

Specific Target

- To ensure that all staff within the Council are aware of the Reuse of Public Sector Information law and that they meet their responsibilities where necessary.
- To develop a re-use of information policy, including disclaimers.
- To investigate the use of an information asset register to categorise and place intellectual value on information.

5. Environmental Information Regulations 2004 (EIR)

All public authorities that are subject to Freedom of Information are also subject to Environmental Information Requests (EIRs). EIR however, also applies to a wider range of organisations or persons who has responsibility for the environment. EIRs therefore include private companies and partnerships with public authorities (water, energy, waste and transport).

The regulations provide a statutory right of access to ALL recorded information about the environment that we hold, subject to certain exemptions to disclosure. This information can be in any format or media; paper, microfilm, microfiche, photos, video, audio, email, computer files, and post-it notes.

A member of the public / organisation can make a request for environmental information by any method - including face-to-face, or by phone.

Specific Target

- To ensure continued compliance with the Environmental Information Regulations by maintaining necessary procedures and processes to deal with 100% of information access requests.

6. Corporate GIS and BS7666

In line with a Corporate Information Assurance Strategy, a Corporate Geographical Information Systems (GIS) Strategy needs to be developed.

The Council requires an overall corporate property systems strategy, and needs to review the system requirements to facilitate the expansion to a Corporate GIS and property based view.

A Corporate GIS system can provide effect the following tangible benefits for the Council;

- A system that will provide members and staff with crucial demographic and policy information that will allow them to readily identify problem areas without the need to trawl through reams of data. This could be data that would identify trends / hot-spots, demographic or crime-related data.

- A system that will facilitate data sharing internally and with our partners i.e. Work that is currently being undertaken with Herts. County, Herts. Police on sharing anti-social behaviour data, noise nuisance and abandoned vehicle data.

- Decreased site visits to elicit data which will be available corporately

- Resources being used effectively. i.e. When a responsive repair is carried out to a property, it will not be repeated under a planned maintenance program

- Decreased property lookup for officers having to search information that may previously have been spread across several departments.

- A system that will allow our citizens to interact more readily in reporting property or land-based problems, especially if browser based GIS wereenhanced on the web-site.

- The provision of a ‘find my nearest’ or ‘points of interest’ in the borough

- A system that will provide consistent and dynamic information across the Council linked to an accurate property gazetteer.

- A system that provides a mini-portal for householders in respect to their property and information associated with it.

- A system that will allow data to published proactively – in line with the Freedom of Information Act 2000

BS7666

BS7666 v7.4 (2012) specifies a standard format for holding details on every property and street. The standard does not differentiate between commercial or residential properties, between occupied, developed or vacant land, between urban or rural or between addressable properties and non-addressable entities such as communications masts.

The use of BS7666 databases brings advantages to the Authority as it makes the sharing of information between internal systems more feasible if they all contain addresses in a common format. In addition, if the partnership working project progresses following the feasibility study, then the potential sharing of property based databases would again be improved if all partners are standardised on BS7666 information.

Specific Targets

- To expand the use of GIS to become a Corporate GIS system
- To appoint an authority GIS Officer and establish the service priorities for GIS, as a base-line exercise, before taking the Corporate approach
- To review current functionality and supplier road-maps for GIS
- To enhance web GIS, and allow better reporting and look-up. To incorporate GIS into the web strategy.
- To maintain the planning land and property database to the BS7666 format to and integrate other systems to use the corporate property gazetteer. The gazetteer should be the 'holistic' view of property through the Council.
- To keep abreast of developments of the BS7666 v7.4 schema and metadata, and insure that the land and property gazetteer data entry conforms to this standard.

Element B – 'ICT Drivers and Solutions'

Introduction

The 'ICT Drivers and Solutions' element of the Protocol should be developed to run in conjunction with the 'Information Assurance' element already detailed. The purpose of this element is to support the objectives of the other strands by identifying the technology requirements they have. It also provides technological solutions to assist the Council and individual departments achieve their aims and objectives.

As has already been identified, the Information Protocol is led by a number of different drivers which include the Organisational Strategy, Audits and Corporate IDP Projects.

In addition, external factors impacting upon the way the service evolves must be considered.

Details

The following service elements have been identified as being important in achieving the key objectives for this part of the Protocol:

Internal Influences

1. Content Management

A content Management System is an essential part in managing the vast amount of information held by any organisation. The system will store catalogue and archive data to allow faster retrieval times and easier access to historical information. The implementation of this type of system would allow improved information sharing by removing barriers between user departments, who could all potentially access a shared corporate repository of information.

Another benefit of any content management system is the ability to devolve the publishing of information to the Corporate Internet or Intranet. This gives users the opportunity to own and manage the information that they publish, so removing a potential bottleneck at the publishing stage.

Specific Target

- To maintain the corporate content management system to assist with the web strategy.
- To devolve the responsibility of information maintenance to user departments across the Council.

External Influences

1. Government Connect4.1 (GCSx)

GCSx stands for Government Connect Secure Extranet. It is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations.
GCSx is connected to the Government Secure Intranet (GSI), which also enables secure interactions between local authorities and central government departments and national bodies. GCSx provides a range of connectivity options to enable access the GSI network and its hosted services; GCSx does not use the Internet or any other public networks.
GCSx provides secure access from connected Local Authorities to many other secure networks such as:

- DWP
- Government Secure Extranet (GSX)
- Government Secure Intranet (GSI)
- National Health Service (NHS)
- Criminal Justice Extranet (CJX)
- Police National Network (PNN)

Specific Target

- To implement all security controls mandated as 'MUST' in Code of Connection v4.1
- To review all security controls currently marked as 'SHOULD' in Code of Connection.
- To insure all staff are aware of their responsibilities for secure connection, including training on remote authentication changes and 'Restricted' data.

2. Shared Services

The shared services project with Aylesbury Vale District Council will look to deliver efficiencies through transformation of aspects service delivery.

Specific Target

- To participate in shared services, and with other partners as appropriate, review ICT Strategy and Information Protocol, Information Sharing Agreements to enable effective delivery of shared or joined-up services.

Document Control

Author:	John Worts - Information Security Manager
Owner:	Steven Baker, Assistant Director – Legal, Democratic & Regulatory
Document Version	1.4
Full Document Title	DBC000 ISS Information Assurance Protocol

Revision History

Revision Date	Previous Revision Date	Previous Revision Level	Summary of Changes	Changes Marked	Next Review Date
June 2009	n/a	0.1	First Draft		
21/6/12	June 2009	1.1	New document to be included as part of IA document structure. Removed references to defunct Pathfinder programme.		June 2013
26/7/12	21/6/12	1.2	Change of title to 'Protocol'. Additional changes to confidential waste and Records Management. References to defunct 2008 ICT Strategy removed		July 2013
2/8/12	26/712	1.3	Comments and amendments post AD meeting July 12. Removed references to Government Gateway – as already established.		August 2014

Distribution List:

Name	Title	Date of Issue	Version

Document Approvals