Basingstoke and Deane

INFORMATION MANAGEMENT POLICY

Title	Information Management Policy
Owner	Head of Law and Governance
Version	1.0 – New Policy 2.0 – Adding Re-use of Public Information Policy 2005 3.0 – Update following changes in senior management 4.0 – Policy Review
Issue date	May 2016
Next revision due	April 2018

Contents

1 MANAGING THE POLICY

1.1 Compliance

All staff, members and contractors or others with access to council information must comply with this policy.

Anyone who is found to have breached this policy could be subject to Basingstoke and Deane Borough Council's Disciplinary and Dismissal Policy & Procedure and serious breaches of this policy could be regarded as gross misconduct.

If you do not understand the implications of this or how it may apply to you, seek advice from Human Resources.

1.2 Advice and Training

If you do not understand anything in this policy or feel you need specific training to comply with it you should bring this to the attention of your manager.

Advice and guidance on all aspects of Information Governance can be found on Sinbad

The Information Governance Officer is able to provide further advice in respect of this policy.

2 INTRODUCTION

2.1 The Information Management Policy sets out the council's obligations in relation to the handling of all information, including information considered to be confidential, sensitive or personal.

2.2 This Policy applies to all information and locations from which council systems are accessed (including home use). Where there are links to enable non-council organisations to have access to council information, the council must confirm the security policies they operate meet our security requirements.

3 PURPOSE AND OBJECTIVES

3.1 The Policy provides guidance to staff and Members on all aspects of information management and brings together the following policies:

- Data Protection Act 1998
- Data Sharing
- Dealing with Data Breaches
- Freedom of Information Act 2000 and Environmental Information Regulations 2004
- Re-use of Public Sector Information (RPSI)
- Information Retention and Disposal
- Government Security Classification Scheme

3.2 In addition, the following Policies are relevant to all staff and Members and have some impact on the use of or access to information:

- Information Security Policy
- Home and Remote Working Policy
- Email Policy

4 ROLES AND RESPONSIBILITIES

4.1 This section sets out the specific roles and responsibilities in relation to good Information Management within the council

4.2 Executive Directors and Senior Managers are responsible for ensuring:

- all staff are aware of and comply with this policy
- all staff are aware of and comply with relevant data handling procedures, which can be found on Sinbad
- suitable data handling procedures are in place within their teams
- all staff have undertaken training as necessary.

4.3 The Head of Law and Governance has undertaken the role of Senior Information Risk Owner (SIRO). The SIRO will take overall ownership of information security, act as champion for information risk at Strategic Leadership Team (SLT) and provide written advice to the Stewardship Team on the content of the council's Annual Governance Statement in regard to information risk. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the council and advises SLT on the effectiveness of information risk management.

4.4 Information Asset Owners (IAOs) have been identified for all Business Units/Service Areas. The role of the IAO is to:

- understand what information is held within their teams, how it is used/transferred, who has access to it and why, in order for business to be transacted within an acceptable level of risk.
- understand and address risks to the information assets they 'own' and provide assurance to the SIRO on the security and use of these assets.

Guidance on the role of the IAO can be found on Sinbad

4.5 The Information Governance Officer is the council's Data Protection Officer and is responsible for ensuring compliance with relevant legislation. In addition, this officer will:

- Ensure the council's notification with the Information Commissioner's Office (ICO) is kept up to date
- Deal with subject access requests made under the Data Protection Act
- Deal with day to day compliance and awareness issues and provide advice and guidance
- Ensure appropriate training is available for all staff and elected Members on Information Governance

4.6 All Elected Members and staff are responsible for complying with this and other relevant policies and procedures covering the use and security of all information and, in particular, personal information.

4.7 All Elected Members and staff are required to notify any security incidents to the IT Manager and the Information Governance Officer in accordance with the Information Security Policy. In addition, staff must notify their line manager immediately an incident has been discovered. Please see Section 7 of the policy for further information on security incidents.

4.8 All contractors, consultants, partners or other agents of the council must:

- Understand the value and sensitivity of council information and treat it accordingly
- Ensure that they and their staff who have access to personal information held or processed for or on behalf of the council are aware of this policy and are fully trained in and aware of their duties and responsibilities under the Data Protection Act. A breach of any provision of the Act will be deemed as being a breach of any contract between the council and that individual, company, partner or firm
- Allow checks to be carried out by the council of personal information held and processed on its behalf to ensure such processing is in compliance with any agreements in place'

- Indemnify the council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation

- Suitable third party processing agreements must be in place before any processing of personal data for which the council is responsible is undertaken by any third party.

5 DATA PROTECTION ACT 1998

5.1 The Data Protection Act 1998 regulates the use of personal information. The council is Data Controller in relation to the personal information it holds on staff, Members and customers. It regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal information lawfully and correctly at all times.

5.2 On 25 May 2018 the Data Protection Act will be replaced with the General Data Protection Regulations (GDPR). Further revisions will be made to this policy prior to the introduction of the GDPR.

5.3 Personal information is defined as information which identifies and relates to a living individual (either by itself or together with other information in the possession of, or likely to come into the possession of the council). It also includes any expression of opinion about that individual

5.4 Sensitive personal data is defined as an individual's:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health condition
- Sexual life

It also includes the commission or alleged commission of any criminal offence and any proceedings for any offence committed or alleged to have been committed.

5.5 The Act sets out eight Data Protection Principles which must be complied with when dealing with personal information. These Principles are legally enforceable:

1. Personal information shall be processed fairly and lawfully and shall not be processed unless certain conditions are met

2. Personal information shall be obtained only for specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes

3. Personal information shall be adequate, relevant and not excessive

4. Personal information shall be accurate and, where necessary, kept up to date

5. Personal information shall not be kept for longer than is necessary

6. Personal information shall be processed in accordance with the rights of data subjects

7. Appropriate measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss, destruction or damage

8. Personal information shall not be transferred to a country outside the European Economic Area less that country ensures an adequate level of protection for the rights and freedoms of data subjects

5.6 Failure to comply with the Principles could result in enforcement action being taken by the Information Commissioner's Office (ICO). Serious breaches could result in a monetary penalty of up to £500,000 being imposed on the council.

5.7 It is a criminal offence under the Act for an individual to obtain, disclose or procure the disclosure of personal information without the consent of the data controller. If a person has obtained personal information illegally it is an offence to offer or to sell personal information

5.8 To comply with the Act the council will:

- Ensure there are legitimate reasons for collecting and using personal information and that such use will be in compliance with the Conditions for Processing as set out in the Act.

- Be clear to customers why we are collecting personal information and what we intend to do with it. This would normally be achieved by providing suitable statements to the customer at the point of collection – for example on our website, as part of a survey or consultation and on application forms.

- Identify the minimum amount of personal information required to provide a service and ensure only that information and no more is collected and retained.

- Take reasonable steps to ensure the accuracy of any personal information obtained. This will include ensuring the source of the information is clear and keeping it up to date where necessary.

- Ensure information is held in accordance with the council's Retention Schedule and disposed of appropriately when required. Disposal should be recorded on Sinbad.

- Ensure the rights of individuals about whom the information is held can be fully exercised under the Act. These include:

    - The right to be informed that processing is being undertaken

    - The right of access to personal information, within the statutory 40 day timescale

- The right to prevent processing in certain circumstances – including for direct marketing
- The right to correct, rectify, block or erase information regarded as incorrect.

- Identify risk areas and ensure appropriate technical and organisational measures are in place to safeguard personal information. This will include the carrying out of Privacy Impact Assessments where appropriate.

- Ensure appropriate security measures are in place, proportionate to the sensitivity of the information held. Further details on information security can be found in the council's Information Security Policy.

- Ensure that personal information is not transferred outside of the European Economic Area (EEA) without suitable safeguards

5.9 In addition, the council will ensure that:

- There is someone with specific responsibility for data protection in the organisation. This is currently the Information Governance Officer

- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice

- Everyone managing and handling personal information is appropriately trained to do so and supervised as necessary

- Procedures are in place to ensure appropriate handling of personal information. Such procedures should be regularly assessed and updated. General data handling procedures can be found on Sinbad, but managers should also ensure procedures relevant to their service areas are also in place.

- The sharing of personal information is carried out under a written agreement, setting out the scope and limits of the sharing. Further details can be found in the Section 6 of this Policy.

- Any disclosure of personal information is in compliance with approved procedures

- Third Party Processing Agreements are in place before the processing of personal information, for which the council is responsible, is carried out by a third party.

- Privacy Impact Assessments (PIA) are carried out at the initial stages of projects which involve the use of personal information or any other activity which could have an impact on the privacy of individuals. Such projects could include:

  - A new IT system for storing and accessing personal information

- a new data sharing initiative
- a proposal to identify people in a particular group or demographic and initiate a course of action
- using existing data for a new and unexpected or more intrusive purpose
- introduction of a new surveillance system (CCTV) or the application of new technology to an existing system (for example adding ANPR recognition capabilities to existing CCTV)
-

Further information on PIAs can be found on Sinbad.

6 SHARING PERSONAL INFORMATION

6.1 Information sharing can include:

- One or more organisations providing information to a third party or parties
- Several organisations pooling information and making it available to each other or to a third party
- One off disclosure of information in relation to a specific purpose
- Sharing of information between different business units or teams within the council

6.2 When seeking to share personal information, the council will adopt and follow the good practice contained within the Information Commissioner's Data Sharing Code of Practice

6.3 Specific guidance on data sharing can be found on Sinbad, including a template Data Sharing Agreement.

6.4 Where a Head of Service considers that a business need exists for personal information to be shared, a suitable Data Sharing Agreement will need to be drawn up and agreed by all parties. This will enable the exchange of information between the council and partner agencies in order to achieve a specific objective.

6.5 The Information Governance Officer will provide advice and guidance to officers who wish to undertake the sharing of personal information and will assist with the production of suitable agreements and procedures.

6.6 In some circumstances, it may be appropriate for internal written procedures to be drawn up to facilitate the exchange of information between business units. Such procedures should incorporate the key points set out in the data sharing template.

6.7 All agreements will be authorised by a manager designated by the relevant Head of Service. The manager will be responsible for ensuring compliance with the agreement and will undertake reviews at appropriate intervals to ensure the purpose for sharing the information remains relevant

6.8 The Information Governance Officer will retain a copy of all agreements and will liaise with the relevant manager to ensure reviews are being undertaken and that agreements remain valid and up to date

6.9 The existence of an agreement or protocol does not give an automatic right to share personal information and all requests must be considered on their own merits

6.10 If a new purpose for sharing arises, which hasn't been notified to individuals at the point of collecting their personal information, we should seek to advise our customers of this. This is particularly important where:

- Sensitive personal information is to be shared
- The sharing may be unexpected or objectionable or may have a significant effect on the individual
- The sharing is particularly widespread
- The sharing is being carried out for a range of different purposes

6.11 In some circumstances it is possible to share personal information without the consent of, or advising the individual concerned. This would normally be where sharing is **necessary** for:

- The prevention or detection of crime
- The apprehension or prosecution of offenders or
- The assessment or collection of tax or duty
- Legal proceedings

Decisions to share in these circumstances must be made on a case by case basis by the appropriate line manager and, where necessary, in consultation with the Information Governance officer. Sufficient information should be retained to provide an audit trail.

6.12 Where sharing of information is as a result of a legislative requirement (for example, housing benefit case information with the Single Fraud Investigation Service (DWP)), procedures should be in place which detail the scope of the requirement and the method of transmission.

6.13 The sharing of personal information with another business unit or section within the council, for a purpose which is not compatible with the original purpose for which the information was collected, must only take place if that use is considered to be fair and lawful. If the purpose is likely to be unexpected or if individuals are likely to object to this use, consideration should be given to informing the individuals concerned.

7 DEALING WITH DATA SECURITY INCIDENTS

7.1 The council has a duty to ensure that all personal information is processed in compliance with the principles set out in the Data Protection Act. It is ultimately the responsibility of each Head of Service to ensure that their service areas comply with that duty. Suitable procedures should be in place for staff to follow when dealing with personal information and all staff must receive adequate training on systems in use within the team.

7.2 The 7th Data Protection Principle requires to the council to take

'appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'

7.3 A security incident may involve:

- Unauthorised persons gaining or seeking to gain access to council premises or those of business partners
- Unauthorised persons gaining or seeking to gain access to the council's information systems whether operated by or on behalf of the council
- Loss, theft, misuse, damage or destruction of any council information asset or equipment
- Computer virus import or infection

A security incident may result in a breach of the Data Protection Act, particularly if, as a result, personal data is compromised.

7.4 The Information Security Policy provides further details, including steps which should be taken to avoid an incident and to follow should an incident or breach occur.

7.5 In the event of personal information being lost or accessed inappropriately, it is vital that action is taken to minimise any associated risk as soon as possible. The process to follow in the event of a breach can be found on Sinbad

7.6 Managers must ensure that all staff are aware of their responsibilities when handling personal information, keeping it secure and not disclosing it without proper cause. Suitable information handling procedures should be in place and all staff must undertake mandatory Data Protection training on an annual basis.

7.7 All staff must take steps to ensure the security of personal information they are handling. As a minimum staff must follow the general data handling procedures which can be found on Sinbad

7.8 In order to keep Members of the Audit and Accounts Committee informed, it is agreed that serious data breaches, where the decision is made to report to the ICO, will be reported to the next available meeting of the Committee. The Committee will also receive a copy of any decision reached by the ICO following its investigation into the breach.

8 ACCESS TO INFORMATION LEGISLATION

8.1 As a public authority, the council is subject to the Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) and is committed to implementing the provisions of the legislation.

8.2 References throughout this policy to FOI will apply to both FOI and EIR.

8.3 FOI allows ***anyone*** to request ***any recorded*** information held by or on behalf of the council. The council must confirm whether it holds the information requested and, if so, release a copy of it within the statutory 20 working days. A limited number of exemptions apply which may allow the council to withhold information

subject to, where necessary, consideration of a public interest test. However, there should always be a presumption to release information requested.

8.4 To comply with FOI the council will ensure:

- As much information as possible is available to the public as a matter of course through the council's Publication Scheme and via the publication of FOI requests and responses as part of a disclosure log
- Where possible, such published information will be in machine readable format
- other information not included in the Publication Scheme is readily available on request, and that such requests are dealt with in a timely manner
- in cases where information is covered by an exemption, adequate consideration is given to whether or not the information should be released and that exemptions are applied consistently
- regard is given to guidance issued by the Information Commissioner's Office (ICO) and any codes of practice issued by the Secretary of State

8.5 Requests received under FOI should be considered without reference to the identity of the applicant or any perceived motive behind the request as release of information is considered to be into the public domain.

8.6 Third parties should be made aware, through any procurement exercise or if they have significant dealings with the council that we are subject to the requirements of FOI and may be required to release information they provide to us.

8.7 It is important that all members of staff are able to recognise when a request for information should be considered under FOI. The Act covers any request for recorded information held by the council. It is not limited to official documents and it covers, for example, drafts, emails, notes, recordings of telephone conversations and CCTV recordings. Nor is it limited to information created by officers working for the council, it also covers, for example, letters we receive from members of the public.

8.8 However, requests for routine information which would normally be provided as part of normal business should continue to be dealt with outside of FOI. This would include, for example, requests for application forms or leaflets or responses to questions staff would normally answer on a day to day basis.

8.9 All requests for information made under FOI will be logged and acknowledged centrally by the Information Governance Officer. Any member of staff who receives a request from a member of the public and believes it should be dealt with under FOI should send it to foi@basingstoke.gov.uk

8.10 The Information Governance Officer will respond to all requests, applying exemptions if necessary.

8.11 The council's process for dealing with FOI requests can be found on Sinbad.

9 RE-USE OF PUBLIC SECTOR INFORMATION REGULATIONS 2005 (RPSI)

9.1 RPSI applies to Public sector information, i.e. information that is produced as part of our public task. 'Public task' means our core role and functions, as defined in legislation or established through custom and practice.

9.2 Re-use means permitting the use of information for a purpose other than the initial public task it was produced for. This may mean an individual, a company or other organisation taking information the council has produced and republishing it or using it to produce a new product or resource.

9.3 RPSI does not apply to:

- Information that would be exempt from disclosure under the access to information legislation – for example, the Data Protection Act, Freedom of Information Act, Environmental Information Regulations or INSPIRE Regulations.

- Recorded information held by the council where someone else holds the intellectual property rights (IPR), for example copyright or database right. We can only permit re-use if we hold the IPR in the information

9.4 Information that is already reasonably accessible, for example if it is on our website, would normally be available for re-use.

9.5 Charges can be made for permitting re-use. In general the only charge permitted is for the marginal costs of reproducing, providing and disseminating the information. For example if a copy of a dataset is provided on disk for re-use we can charge for the cost of the disk and postage. The exceptions to this concern public sector bodies required to generate revenue to cover:

- A substantial part of the costs relating to their public task

- Documents for which the public sector body is required to generate revenue to cover a substantial part of their costs

It is unlikely charges can be made for information published on our website or released under the Open Government Licence.

9.6 If any member of staff receives a request to re-use information, please forward it to the Information Governance Officer.

10 INFORMATION RETENTION AND DISPOSAL

10.1 This section covers all recorded information held in all formats, including:

- emails
- Post-It notes
- electronic and paper documentation
- images and photos, including CCTV
- maps and plans
- databases and spreadsheets
- telephone conversations
- electronic systems data records

- video and audio recordings
- web and social media (e.g. twitter) content

10.2 The 5th Data Protection Principle states personal information must not be kept for longer than is necessary. This means, retaining documents or records that contain personal information beyond the length of time necessary for the purpose for which that data was obtained is unlawful

10.3 The council's Retention and Disposal Schedule sets out the statutory retention periods of information processed by the council. Where no statutory retention period exists, information will be retained for two years. If there is an operational need for information to be kept for a longer or shorter period this exception must be agreed with the relevant head of service and recorded on the Retention and Disposal Schedule. The schedule can be found on Sinbad.

10.4 Where a retention period has expired in relation to particular information a review should always be carried out before a final decision is made to dispose of that information. Ultimate responsibility for determining whether to retain or dispose of specific information rests with the Head of Service in respect of information that falls within the remit or control of their service.

10.5 The council performs regular backups of electronic information for disaster recovery purposes. This backup process operates on a 90 day cycle, so although electronic information may have been disposed of and recorded as such, any backup of that information will remain for a further 90 days before full and permanent eradication.

10.6 The council has a duty to continue to be able to retrieve the information it stores. The rate of technological changes means that the form and format of storage media is continually changing, giving it a finite life. Even when information remains intact, the continued availability of devices to read it can't be assumed. Consideration, therefore, needs to be given to the issue of long term storage and retrieval of electronically held information. Adobe's Portable Document Format/Archive (PDF/A) file format is currently the ISO standard for ensuring that electronic documents can be reproduced in exactly the same way in years to come. It is particularly important when securing software to ensure future availability of information.

10.7 Heads of Service are expected to be proactive in carrying out or instigating regular reviews of existing information that may be suitable for disposal.

10.8 Disposal of information must be by the most appropriate method. Where possible, paper based information should be recycled

10.9 Paper information containing **personal, sensitive or confidentia**l information must be disposed of via the confidential waste bins. Failure to adhere to this instruction may result in the unauthorised disclosure of such information to third parties and render the council liable to enforcement action under the Data Protection Act 1998.

10.10 Transfer of information to a third party is unlikely to be an option in most cases where there is personal data having regard to the Data Protection Act 1998. However, this method of disposal will be relevant where information or records

are of historic interest and/or have intrinsic value. The third party could be the County Archivist or a local Museum.

10.11 ICT systems should be able to permanently delete information at the end of the relevant retention period. The ability to retain and delete information in accordance with this policy should be a major consideration at the outset of any proposal to purchase an ICT system.

10.12 Disposal of all information listed on the Retention Schedule should be documented using the Disposal Log which can be found on Sinbad by following the link below:

Disposal Log

To update the log, click on 'New item' and complete the template.

Please note, information disposed of in the normal course of business does not need to be recorded on the disposal log. Further guidance on retention and disposal can be found on the Information Management pages on Sinbad.

11 GOVERNMENT SECURITY CLASSIFICATION SCHEME

11.1 Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. The three levels of classification are:

11.2 **OFFICIAL**

OFFICIAL is the classification which will apply to the majority of information created or held by the council.

All routine council business, operations and services should be treated as **OFFICIAL** and the council operates almost exclusively at this level. This includes:

- The day to day business of the council
- Public safety, criminal and enforcement activities
- Most aspects of security, resilience and emergency planning
- Commercial interests, including information provided in confidence and intellectual property
- Personal information that is required to be protected under the Data Protection Act 1998

ALL council information must be handled with care to prevent loss or inappropriate access and deter deliberate compromise or opportunist attack

Staff must understand that they are **personally responsible** for securely handling any information that is entrusted to them in line with local business processes

Baseline security controls reflect commercial good practice

There is no requirement to mark **OFFICIAL** information.

A limited subset of **OFFICIAL** information could have more damaging consequences (for individuals, the council or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the "**OFFICIAL"** classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the need to know. In such cases where there is a clear and justifiable requirement to reinforce the need to know, assets should be conspicuously marked: "**OFFICIAL– SENSITIVE"**

Managers will identify any sensitive information within this category, based on a risk matrix. All information considered to be 'very high risk' will be classed as **OFFICIAL – SENSITIVE**. The risk matrix must contain procedures and guidance for the handling of information falling under this category. Information Risk Assessments will be undertaken by each business unit and made available on Sinbad. Reviews should be undertaken in line with the annual service planning exercise.

OFFICIAL – SENSITIVE should only be used where the sensitivity of the information justifies strict restrictions on information sharing. For example:

- where there is a bulk transfer of personal details that would require the use of secure, PSN email. This would include information such as benefits, financial returns or electoral registration details.

- for certain commercial or market sensitive information which could prove damaging to the council or a commercial partner if improperly accessed

- for particularly sensitive personal information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, or vulnerable individuals.

These enhanced controls will effectively manage associated confidentiality, integrity and access risks and need to be carried out on a case by case basis

Special handling instructions are an additional way to identify particularly sensitive items that require additional protection, limit access and enhanced handling and storage

11.3 **SECRET**

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat factors. For example, where compromise could seriously damage military capabilities, internal relations or the investigation of serious organised crime.

Consideration should be given as to whether any information held by the council would fall under this category, but it is likely to be limited to information on known Government or military establishments or, possibly, some emergency planning information.

11.4 **TOP SECRET**

HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause

widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

It is unlikely the council will hold any information in this category

11.5 Further guidance on the Government Classification Scheme, including the four key principles, will be added to the Information Management pages on Sinbad shortly.