BCP Council
Information Governance Policy

1. Why do we have this policy?

Reason

BCP Council recognises the need to fully comply with the requirements and obligations of the:

- Human Rights Act 1998 (HRA)
- Data Protection Act 2018 (DPA)
- Common law duty of confidentiality
- Privacy and Electronic Communications Regulations 2003 (PECR)
- The Computer Misuse Act 1990
- Protection of Freedoms Act 2012 (POFA)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Freedom of Information Act 2000 (FOIA)
- Environmental Information Regulations 2004 (EIR)
- Copyright, Designs and Patents Act 1988
- General Data Protection Regulations 2016 (GDPR)

The Council generates and receives large quantities of information. It recognises that information is one of its key corporate assets and that it has a responsibility to protect and, where required by law, provide and publish information.

Purpose

This policy will provide a consistent approach for all Council staff as it collects and processes information from individuals, organisations and employees.

The policy will ensure the correct and lawful handling of all business and personal information as an essential part of both Council's service delivery. The Council will fulfil the legal obligations under all relevant legislation and comply with recommended good practice from the Information Commissioner's Office embodied in Codes of Practice and other guidance.

Information is a key resource for the effective operation and accountability of the Council. Like any other asset, it requires management. This policy sets out the principles that the Council has adopted for the management of their information assets. The Council recognises that some of its records will become of historical value. Such records will be

transferred to the Dorset Archive Centre, in line with the Joint Archiving Service agreement.

2. Who must comply with the policy?

All staff, contractors and elected members and any other persons engaged in the Councils' service delivery must comply with this policy.

3. Who needs to be aware of this policy externally?

Partner organisations, contractors, consultants and any other persons engaged in Councils' service delivery.

4. What is the policy?

Access to business information (under the FOIA/EIRs)

The Council is committed to an access to business information framework that ensures:

- Business information that should be made publicly available by law is published on the BCP Council website to meet the requirements of the FOIA and the Local Authority Transparency Code 2015
- All requests for information are dealt with within the statutory timescales and where any delays are anticipated applicants are regularly kept informed of progress
- Advice and assistance is offered to help any enquirer frame their request so that they receive the information they require
- Requests are assessed to ensure the confidentiality of personal or commercially sensitive data is not breached, disclosure is in the public interest and provision of the information is not prejudicial to the provision of essential Council services
- Information is withheld if legitimate exemptions apply and the application of the exemptions are adequately explained
- All enquirers are advised of their rights to question the information received and know what has not been provided and why
- Prior to deeming requests vexatious or manifestly unreasonable, all previous requests and relevant history of the requestor's complaint communications with the Council will be considered. The advice of the IG Team must be sought prior to deeming a request vexatious or manifestly unreasonable
- All enquirers will be advised of their right to request an internal review via the Councils' complaints procedure if they are dissatisfied with a response to a request and of their right to refer the case to the Information Commissioner if they are dissatisfied with the outcome of an internal review
- All requests will be monitored and performance indicators made available to demonstrate compliance with the legislation
- All staff will be provided with suitable awareness training and guidance, so that they recognise and know what to do if they receive a request for information

Looking after personal data

The Council will comply with the Human Rights Act, the principles of the Data Protection Act 2018 (DPA), General Data Protection Regulations 2016 (GDPR) and the common law duty of confidentiality (see Appendix A). They are committed to a framework that ensures personal data is:

Used fairly, lawfully & in a transparent manner

- The Council will only hold personal information where it is justified to do so
- The Council will ensure that it has privacy notices that adequately explain the purpose for obtaining, using and sharing information. Wherever possible such notices will be published on the Council's website
- The Council will seek consent to process only where necessary and will consider alternative lawful basis before using consent
- Where consent is not required the Council will ensure that it has a robust lawful basis to process personal data and that it meets a condition, or conditions for processing

Used for specified, explicit & legitimate purpose

- BCP Council is Data Controller for its data. Personal data held by the Council can be used as permitted by law and in accordance with the privacy notices
- All access to the Council's data will be on a "need to know" basis and appropriate security and access controls will be in place so only staff that need access to the personal data will be permitted access to it
- Sufficient management checks and audit checks will be in place to ensure personal information is not processed in a manner that is not compatible

Adequate, relevant & necessary

- The Council will only hold the minimum personal information necessary to enable it to perform its functions

Accurate & up to date

- The Council will endeavour to ensure information it holds is accurate and up to date
- The Council will ask individuals to keep them informed when a change of circumstances leads to a requirement to update information
- The Council will periodically assess information for accuracy and relevance

Not kept longer for than necessary

- The Council will dispose of information when it is no longer needed for the purpose, or purposes for which it was obtained
- To meet this requirement Service Units will develop and maintain retention and disposal schedules for their service delivery areas, taking into consideration any statutory requirements
- Personal information will be anonymised, pseudonymised or not kept in a form which identifies the data subject, for longer than is necessary

Held and processed securely

- The Council will ensure it has systems in place to keep information secure
- All persons subject to this policy must refer to the Information Security Policy for the Council

Registration/notification to Information Commissioner
The Council will ensure annual registration fee will be paid to the Information Commissioner's Office (ICO). The Council shall maintain an Information Asset Register for every area of service delivery, detailing the Council's data processing, data sharing and retention. These registers will be available to the Information Commissioner on request.

Special category personal data

- The Council will ensure that it adheres to the additional requirements to protect and secure special category personal data, as defined by the DPA 2018 which includes the GDPR
- Special category personal data will normally only be disclosed to third parties with the consent of the data subject
- The Council will ensure that where consent is not required it will still endeavour to be "fair" and to advise the data subject about disclosure, unless this would prejudice the purpose of the disclosure
- The Council will ensure that where special category personal data is disclosed without consent, that it is permitted and justified by law to do so. This decision will be made at senior management level with advice sought from the Head of Information Governance or Principal Information Governance Officer
- The reasons for disclosure will be recorded

Rights for data subjects

Used and provided in accordance with the rights of individuals
The Council will recognise the rights given to individuals under the DPA, including the absolute right to access information (subject access), the right to have inaccurate information corrected or erased, and the right to entitlement to compensation should any damage be suffered as a result of any breach of the Data Protection Act 2018 and GDPR principles

Access by individuals to their personal data

- All requests by individuals to access their personal data (subject access request - SAR) must be sent to the Information Governance Team
- The Council procedure for dealing with subject access requests will meet the legal requirements of the Data Protection Act 2018 and the Information Commissioner's Office (ICO) Code of Practice
- The Council will provide a subject access request form on the Council's website to assist with requests
- All requests will be logged, tracked and monitored. Requests will be directed to relevant Service Unit Information Asset Advisor to process
- In accordance with the ICO Code of Practice, the Council will only ask for identification if the request cannot be validated from existing data it holds
- The Council will endeavour to respond to all requests within the statutory time limit of 30 calendar days. Where deadlines cannot be met, individuals will be kept informed
- The Council will endeavour to assist customers who make a verbal request to put the request in writing
- Exemptions to the right of access under the DPA will be applied fairly and consistently

- If an exemption is considered to apply, the decision not to disclose information must be subject to advice from the Information Governance Team, in consultation with the Service Unit, and the reasons for non-disclosure documented
- In considering whether to disclose information, the Council will take care not to reveal the identity of other third party individuals. Any information supplied by a third party deemed to be provided in confidence will not usually be disclosed without first seeking permission from the source

Provision of unstructured personal data

- "Unstructured personal data" means any personal data which relates to an individual but is not referenced or structured to that individual
- If the cost for the provision of unstructured data will exceed the fee limit prescribed in the FOIA & Data Protection (Appropriate Limit & Fees) Regulations 2004 the Council can refuse the request. The current fee limit is £450, which equates to 18 hours officer time.

Requests made on behalf of children

- A request for information may be made by a parent, guardian or other responsible adult authorised to act on behalf of a child
- Persons acting on behalf of a child may be required to verify that they have parental responsibility or the consent of the child (where the child is old enough to provide consent)
- Information will not be disclosed to a third party where to do so would clearly not be in the child's best interests. This includes information requested on the child's behalf by a parent or person with parental responsibility. The decision to withhold information will be made by the relevant senior manager, in consultation with the Information Governance Team. Reasons for non-disclosure will be documented

Requests made by children

- Any child may be allowed to see their own records unless it is obvious that they do not understand the implications and potential consequences of doing so. The Council will apply the Gillick Competency and Fraser Guidelines.
- Information will not be disclosed to a child, where this is likely to cause serious harm to their physical or mental health. The decision to withhold information will be made by the relevant senior manager, in consultation with the Information Governance Team. Reasons for non- disclosure will be documented

Right to be informed

The Council will publish a corporate Privacy Notice and specific Privacy Notices for Council services detailing processing conditions, data sharing and retention periods. Individuals will can enquire about the specific use of their data with each area of service delivery and they can write to the Council's Data Protection Officer regarding the application of the law and the Councils' Policy.

Right to rectification

The Council will consider and respond to any requests from data subjects to have their personal information amended within one month. If a request is refused, or part refused, reasons will be documented. The decision in regard to a request will be made by a senior member of staff in the relevant Service Unit, in consultation with the IG Team. Decisions will be documented by the relevant Service Unit.

Right to erasure/right to be forgotten
The Council will consider and respond to any requests from data subjects to have their personal information erased within one month from receipt. If a request is refused, or part refused, reasons will be documented. The decision in regard to a request will be made by a senior member of staff in the relevant Service Unit, in consultation with the IG Team. Decisions will be documented by the relevant Service Unit.

Right to restrict processing
The Council will consider and respond to any requests for the restriction or suppression of their personal information by the data subject within one month. If a request is refused, or part refused, reasons will be documented. The decision in regard to a request will be made by a senior member of staff in the relevant Service Unit, in consultation with the IG Team. Decisions will be documented by the relevant Service Unit.

Right to data portability
The Council will respond to any requests for information to be supplied to the data subject or supplied to an organisation nominated by the data subject within one month. The Council will ensure information can be moved, copied or transferred in a safe and secure way.

Right to object
The Council will consider and respond to any requests to object to the processing of personal information by the data subject within one month. The Council will comply with the law and best practice advised by the Information Commissioners Office for processing personal information for the purposes of direct marketing. If the request is refused or part refused, reasons will be documented.

Other Rights of the Individual

- This policy shall not affect or in any way compromise an individual's rights under the Human Rights Act 1998 (HRA)
- An individual's right to privacy is protected under the Freedom of Information Act by virtue of exemption. Personal data will not be disclosed as part of an FOI request if to do so would breach any of the principles of the DPA

CCTV Requests

- Requests for CCTV footage should be submitted in writing and sent to the CCTV Manager or the Information Governance Team
- Where a commercial company or organisation (e.g. solicitor, insurer, housing association) is acting on behalf of a requester, the Council will charge a non-refundable fee of £75

Disclosure of personal data without consent and/or knowledge of data subjects
The Council is legally permitted to disclose personal data without the consent and/or knowledge of data subjects under certain circumstances. These reasons are defined as exemptions under the DPA. It will apply exemptions fairly and consistently in accordance with the Act. Exemptions will be carefully considered on a case by case basis.

- By Order of the Court (a Court Order), or for the purposes of legal proceedings

- Where the purpose of disclosure is to enable the Council to assess or collect any tax or duty or any imposition of a similar nature
- Where the purpose of disclosure is to prevent or detect a crime, apprehend or prosecute offenders
- Where the purpose is to protect any person who is at risk of serious harm
- Where there is an obligation by law to disclose information, for example a statutory request by another public sector body with enforcement powers. Statutory agencies include the HMRC, Asylum & Immigration, HM Customs & Excise, etc.
- Where information is required for research purposes, providing such data is general and does not cause damage or distress to the data subject
- Where disclosure is to safeguard national security
- Where the purpose of disclosure is to enable elected members to fulfil their Council functions, for example where the Councillor is a member of a specific committee, or when acting in their ward capacity on behalf of a constituent

Disclosure requests from third party agencies

- All requests for information from public bodies or other third party agencies must be in writing, other than where immediate action is required by public bodies to meet urgent requests. Such requests must be followed up in writing as soon as possible
- Other third party agencies (not public bodies) include members of a data subject's family, legal representatives of a data subject, a data subject's employer and any organisations acting on behalf of an individual such as the Citizen's Advice or a Housing Association
- Where a public sector body or other third party agency seeks to rely on a legal authority (legislation) for disclosure, they must provide sufficient detail to explain how the legal authority applies to the request
- Personal data will not usually be disclosed to other third party agencies without the written consent of the data subject (authority to disclose document)
- In accordance with the Data Protection Act, a 30 day time limit will be applied to requests for data from other third party agencies, including the requirement to inform of any decision to withhold information and the reasons for doing so. This decision will be taken by a senior member of staff and the reasons for not disclosing documented and made clear to the other third party agency
- Information will be not be disclosed where this is likely to cause serious harm to a vulnerable child or adult's physical or mental health. In all requests for access, the interests of the subject, particularly in the case of a vulnerable child or adult must be paramount and the duty of the Council to protect vulnerable children and adults from potential harm of primary importance

Disclosure requests for the purposes of crime prevention (DPA & GDPR)

- Requests will usually be from the police, but may be received from other public sector regulatory bodies
- Requests should be submitted in writing
- Requests for information should be directed to the appropriate Information Asset Advisor or the Information Governance Team
- Police officers should submit requests in writing, countersigned by their superior officer and using documentation relevant to their Police Force. Dorset Police use form A232
- Council officers must seek the immediate advice of the IG Team if they are in any doubt about disclosing information in response to an urgent, verbal request under DPA 2018

Disclosure requests for the purposes of legal proceedings (DPA & GDPR)

- Requests under DPA/GDPR should be submitted in writing or where applicable, with a copy of the relevant Court Order
- Requests for information under DPA/GDPR should be directed initially to the Information Governance Team
- Where a commercial company is acting on behalf of a requester, the Council will charge a non-refundable administration fee of £75 per DPA/GDPR request

Use of personal data for marketing purposes

- The Council will comply with the Privacy and Electronic Communications Regulations (PECR).
- Personal data collected by the Council will only be used for marketing purposes where customers have been told this will happen via a privacy notice (PN) and customers have consented to receive such information.
- All emails sent to customers for marketing purposes will include a 'how to opt-out' message.
- Databases used by BCP Council for marketing purposes will be 'cleansed' at least every two years to determine whether customers still wish to receive information and to verify the accuracy of the data.

Privacy Impact Assessments (PIA)

- The Council will, where applicable, undertake PIAs within its policy development and project management frameworks in order to ensure that the potential impact of any new developments on the privacy of individuals has been effectively considered and risk assessed

Ensuring Data is transferred appropriately

- The Council operates its own website which are accessible by countries outside the European Union (EU) and which involves the transferring of data on an international basis. The website provides structured information about BCP Council, their staff and the services provided. Where personal data regarding individuals is published on the website, written consent from data subjects must be obtained prior to any personal details being published
- The Council may need to transfer data to another country. If this situation arises, the necessary enquiries will be made as to whether the transferee country has adequate data protection. If not, information will not be transferred unless there is a legal obligation to do so. However, data can be transferred to any country, even if outside the EU, if the data subject has given his/her consent

Information sharing with partner agencies

- The Council recognises that information sharing helps to improve service delivery and protect vulnerable members of the community, both adults and children. It is also essential to facilitate the delivery of services within the partnership frameworks that are developing and will continue to develop within the foreseeable future.
- The Council will ensure that information sharing is conducted within a robust framework, based on the Dorset Information Sharing Charter (DISC) and Personal Information Sharing Agreements (PISAs).
- The Council will share information fairly and lawfully and will respect the rights of individuals in line with information rights legislation, the DISC and supporting PISAs

- The IG Team will maintain a Register of Information Sharing protocols. Regular review of protocols will be effected by the team and/or responsible lead managers in order to ascertain their continuing validity.

Caldicott Guardian

- The Council will apply the Caldicott principles and processes, which provide a framework of quality standards for the management of personal and/or confidential information within Health and Social Care services
- The Council will publish the names of its Caldicott Guardian(s) on the Council website
- The Caldicott Guardian will be informed of any information security breaches or incidents involving social care information and will in consultation with the Head of Information Governance agree any remedial action required to mitigate risks

Information security

- Personal data and/or confidential data will be handled in accordance with the Council's Information Security policy
- Employees working from home with access to manual or electronic data are responsible for ensuring the safety and security of such data in accordance with the Council's Information Security policy
- Any information security incident or breach must be reported immediately to the responsible manager and the Information Governance Team

Information/records management

Good information management is vital to ensure the effective and efficient operation of the Council's services. The Council recognises the value of its information assets and will ensure that these assets are managed effectively, in accordance with the following principles. These reflect the legislation and professional standards and principles attached at Appendix B.

The Information Governance Team and Strategic IT will provide advice and guidance to all Service Units regarding management of their information and records in accordance with legal requirements and good practice guidelines.

- All information has a defined owner(s). It will be the responsibility of Service Directors in their capacity as Information Asset Owners to manage, protect and make it available to others. Information Asset Owners will appoint Information Asset Managers to assist them with their responsibilities.
- Service Units will maintain an Information Asset Register.
- Sufficient, accurate and timely information will be available to the business processes that require it.
- Information will be made available unless there is a compelling reason not to do so, recognising all the relevant legislative and regulatory requirements. This applies to both internal and external users of information. Efforts will be made to present and organise information to maximise its availability and usefulness.
- The storage and organisation of information will promote its sharing, thereby minimising duplication of effort and the cost of its retrieval, as well as contributing to improved decision making.
- The protection of all information assets will be undertaken in accordance with Council's Information Security Policy.

- Information Asset Owners will also include information risks within their Annual Governance Statements.
- The management and retention of information will take into account its value to the Council. Information will only be retained in line with statutory legislation and/or as long as there is a business requirement, in accordance with Service Unit Retention & Disposal Schedules.
- Disposal of information of a personal or confidential nature will be carried out securely.
- Information ownership rights will be observed. Information from third party sources will only be used in accordance with the licence or permissions granted. Equally, the intellectual property rights of the Council will be considered in relation to the distribution of its own information assets.

The cost of retaining and managing information will be minimised by the appropriate use of available processes, equipment and technologies.

The Council will manage the flow of data and information to users and processes using IT Business Systems and such overarching/underlying technologies as the Customer Relationship Management system (CRM) and Microsoft Office 365. This will ultimately result in a formal Information Architecture to manage information across the organisation from front-office customer-facing systems to strategic and back-office IT systems

Access to records/information

The Council recognises the need for consistent information to be available in ways that suit users and customers. The Council will ensure that decisions regarding access to records are documented so that they are consistent, and can be explained and referred to.

Service Directors in their capacity as Information Asset Owners will ensure that:

- All staff have access to the records/information they require access to in order to perform their roles and responsibilities
- All staff and managers are aware of the arrangements for requesting and/or permitting access to certain types of information and have attended all the mandatory IG training courses
- Procedures are in place to document decisions concerning access
- Access to records/information is regularly audited

Organisation of records/information – electronic and manual records (including email)

Service Directors in their capacity as Information Asset Owners will ensure that Service Unit information is held in an organised and indexed structure to reflect logical groupings of records and to provide for quick and efficient discovery and retrieval by all relevant officers who are authorised to access the information. They will maintain their Information Asset Register of their information and records. The file/folder structure, within a shared drive or drives or other electronic environment, or within a manual filing system, will define the principal classes of information reflecting the functions of the Service Unit, sub-divided into more detailed sub-classes to represent the business activities and transactions within the relevant function.

The file/folder structure will facilitate the application of access controls and the retention and disposal of information.

Records/information received via the Council's email systems that should form part of the Council's permanent information/record systems will be transferred and saved by staff into Service Units organised and indexed file/folder systems (electronic or manual) or line of business databases, where this functionality exists and it is the appropriate location to store it. Emails should not be permanently stored within Council's email systems. Email systems are for the purposes of communicating information; they do not have the functionality to organise or manage information for the purposes of shared access, discovery, retrieval, further processing or retention and disposal.

In the case of "line of business" application systems (customer/property databases, etc.), the file/folder scheme will incorporate the existing structure of the information. Typically, such information is stored under a unique identifier, either a person (such as a service user) or a physical structure (such as a property). Service Unit electronic systems will be capable of:

- arranging and indexing records in such a way that they can be retrieved quickly and efficiently
- the creation of records with the addition of descriptive tagging (metadata) necessary to document business processes: this should be part of the systems which hold the records
- the secure maintenance of the integrity of electronic records
- the accessibility and use of electronic records for as long as required (which may include their migration and access across systems)
- the application of appropriate disposal procedures, including procedures for archiving; and the ability to cross reference electronic records to their paper counterparts in a mixed environment.
- Creating backups of electronic records to ensure continuity in the event of record loss, damage or destruction
- audit trails, which must be held securely and made available for inspection by authorised personnel.

Maintenance of records/information

Record keeping systems must be maintained so that the movement and location of records are monitored. This includes:

- Controlling access to the information
- Ensuring authenticity, so that records retain their legal integrity
- Identifying vital business records and applying the appropriate protection, including a recovery plan that ensures the restoration of the business function
- Identifying records no longer required for business purposes and where appropriate transferring to designated storage in line with Service Unit Retention and Disposal schedules

Retention & disposal of records/information

Information Asset Owners will ensure that Service Unit retention and disposal schedules are developed, applied, maintained, reviewed and updated in line with legislation and good practice guidelines.

If there is no legal requirement to keep information it will be destroyed as soon as it is no longer required for the business purpose that it was created for, in line with Service Unit Retention and Disposal schedules. Information will not be held for longer than it is relevant to the purpose for which it was obtained.

Data Quality

- The Council recognises that the quality of the data that it holds is key to delivering effective and efficient services. 'Bad' data imposes a cost to the Council to cleanse, limits opportunities to deliver services, affects the decisions that it makes and impacts on its ability to share information internally and externally.
- Data quality will be considered from the lowest level of entry into the Council, ensuring that quality data is used to support all levels of Council business. Correcting data as close to the point of collection provides the most cost effective method of providing for high quality data to business systems, and to our partners and the public.

Complying with the Legislation

- The Council will have nominated staff (Information Asset Advisors) within all of its Service Units to provide information governance advice and to support the Council's IG framework
- The Information Governance Team will provide more detailed and specific advice to staff, councillors and the Council on all matters relating to information compliance legislation and the wider information governance function
- Basic Freedom of Information and Data Protection/GDPR training is mandatory for all staff and will be provided through e-learning packages maintained by the Information Governance Team and/or face-to-face induction training.
- Freedom of Information and Data Protection/GDPR awareness training sessions will be included in the annual corporate training programme. Bespoke, Service Unit training updates will also be provided in accordance with the IG Team training programme
- The Information Governance Team will notify staff of changes to Freedom of Information and Data Protection legislation, how these changes will affect them, when they will occur and what is required to stay within the law.
- All councillors will undertake councillor training in Freedom of Information and Data Protection legislation and associated Council policies
- The Information Governance Team will ensure the notification fees are paid to Information Commissioner Office
- The Head of Information Governance can refer Service Units that are causing concern in respect of information rights legislation compliance to the Information Governance Board and Audit & Governance Committee
- The HoIG will report on the Council's information governance function to the Audit & Governance Committee at regular intervals
- The IG Team will prepare performance management information reports for Service Directors and Information Asset Advisors no less than quarterly, so that compliance in respect of requests for information under information rights legislation is effectively monitored.
- The Council will investigate any breach of information rights legislation and this policy. Staff will be trained in reporting and managing information security breaches.
- If a breach meets the reporting criteria as set out by the Information Commissioner's Office, the Council will self-report to the Information Commissioner's Office. The Council will implement any actions the Information Commissioner directs it to take as a result of its assessment or investigation.

- The IG Team will provide advice and support, so that councillors comply with the legal requirement to notify the processing of personal data that they obtain, use and store in their ward capacity, to the Information Commissioner.

Complaints
The Council will use the Council's complaint procedure to acknowledge and resolve any complaints or issues made by external customers.

The Council will respond appropriately to any ICO complaints with regard to the Data Protection Act 2018/GDPR, Freedom of Information Act or related information governance issues.

5. How is this policy implemented?

Through staff procedures, processes and guidance which are published to the IG pages of the Council's intranet service, Service Unit Information Asset Advisors who provide advice and guidance within their Service Units, e-learning packages and the delivery of training and provision of advice by the IG Team.

Procedures

Procedures, guidance and details of IG training services are available on the intranet.

Roles and responsibilities

The **Chief Executive** is legally responsible for compliance with this policy and legally liable in the event of any failure to comply with the policy.

The **Senior Information Risk Owner (SIRO)** is responsible for promoting and encouraging compliance with this policy by all senior managers, as part of managing the Council's information risks

The **Caldicott Guardian** is responsible for promoting and encouraging compliance with this policy within social care areas of service delivery, as part of protecting the confidentiality of service user social care information

Information Asset Owners (Service Directors) are responsible for managing, protecting and making information in their ownership available to others.

Information Asset Advisors are responsible for promoting and monitoring compliance with this policy and providing information rights and information management advice and guidance to staff within their respective Service Units

All Managers are responsible for implementing and enforcing this policy.

Every Employee must abide by this policy. Failure to comply with this policy may result in disciplinary action. Anyone contravening the Freedom of Information Act 2000 and/or Data Protection Act 2018 (GDPR) can be held personally liable and face court proceedings for certain offences, which may result in a fine and /or a criminal record.

Every Councillor must abide by this policy. Failure to comply with this policy may represent a breach of the Councillor Code of Conduct and be subject to referral to the Standards Committee. Anyone contravening the Freedom of Information Act 2000 and/or Data Protection Act 2018 (GDPR) can be held personally liable and face court proceedings for certain offences, which may result in a fine and /or a criminal record.

The Council's Information Governance Team will provide advice and guidance to all persons to whom this policy applies in respect of compliance with information rights legislation and the wider information governance function, which includes the Data Protection Act 2018 & Freedom of Information Act.

Suppliers and **Partners** must agree to abide by this policy as part of their contractual obligations.

Enforcement

Non-compliance with this policy will be enforced by managers and where applicable through the Council's disciplinary policy and procedures.

6. Supporting information

Further information on the legislation and guidance is available from the Information Commissioner's office website www.ico.gov.uk

Effective from date	April 2019
Review date	April 2021
Review frequency	Two years
Policy Owner (job title)	Head of Information Governance
Policy Author (job title)	Principal Information Governance Officer
Policy Sponsor (job title)	Service Director, Legal & Democratic
Approval bodies	Information Governance Board, Corporate Management Team (CMT)
Approval dates	
Related legislation	Data Protection Act 2018 Freedom of Information Act 2000 Human Rights Act 1998 Regulation of Investigatory Powers Act 2000 Environmental Information Regulations 2004 Protection of Freedoms Act 2012 Common law Duty of Confidentiality Privacy and Electronic Communications Regulations 2003 General Data Protection Regulations 2016
Related policies	Information Security Policy
Version	V1.0

Revision history

Version	Date	Amendments made	Requested by (job title)	Made by (job title)

Consultees

Name	Organisation	Date consulted
Service Directors (Information Asset Owners)	BCP	
Corporate Policy & Strategy Officer	BCP	
Information Asset Advisors	BCP	
Head of Strategic IT	BCP	
Head of Strategic HR	BCP	
Senior Information Risk Owner & Deputy SIRO	BCP	
Caldicott Guardian	BCP	
Equality & Diversity Manager	BCP	
Head of Audit & Management Assurance	BCP	
Consultation & Market Research Manager	BCP	

Equality Impact Needs Assessment

Assessment date	

Freedom of Information Act Exemption

FOI Exempt	

APPENDIX A

INFORMATION RIGHTS LEGISLATION

Human Rights Act 1998 (Article 8)

Everyone has a right to respect for his private and family life, his home and his **correspondence**

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others (legitimate aims)"

The Article 8 right is a **qualified** right and permits public authority intervention when this is:

- in accordance with law,
- in the pursuit of a legitimate aim,
- necessary in a democratic society

Common law duty of confidentiality

Information provided in confidence by a third party is protected under the common law duty of confidentiality, subject to the public interest test.

For personal information to have the necessary quality of confidence it:

- Is not in the public domain or readily available from another source
- Has a degree of sensitivity
- Is communicated for a limited purpose and in circumstances where the individual is likely to assume an obligation of confidence, e.g. health practitioner/patient, banker/customer, solicitor/client, social worker/service user, etc.

Data Protection Act 2018 (GDPR 2016)

The Act incorporates the General Data Protection Regulations 2016 and updates the previous Data Protection Act 1998. It governs and regulates how personal information is used. The Act defines six principles, which the Council must adhere to. A breach of any of the principles is a breach of the law.

Personal information/data is information about a living individual, who can be identified from that information.

Special category personal data is defined in the Act as:

- racial or ethnic origin
- political opinion
- religious belief
- union membership
- physical/mental health
- sexual life
- genetic/DNA
- biometric

There are additional requirements placed upon the data controller for the processing of special category personal data.

A *data subject* is the individual who the personal information is about. A *data controller* is the organisation/company legally accountable for the personal data that it obtains, uses, holds, etc. BCP Council is the Data Controller for the personal data it processes. A *data processor* is an individual or organisation that processes personal information on behalf of a data controller and under the instruction of the data controller.

The Act specifies the lawful conditions for holding and processing criminal offence data in an official capacity or under specific legal authorisation.

Privacy & Electronic Communications Regulations 2003 (PECR)
The Regulations sit alongside the Data Protection Act. They give people more privacy in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes
- cookies (and similar technologies)
- keeping communications services secure
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings

Protection of Freedoms Act 2012
The Act enhances individuals' privacy rights in some areas. These include CCTV surveillance and processing biometric data.

Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIRs)
The Freedom of Information Act and Environmental Information Regulations give people the right to ask for access to recorded information held by the Council.

Some business information held by the Council will be subject to exemption from disclosure under these Acts.

Computer Misuse Act 1990
The Computer Misuse Act defines a number of criminal offences, relating to hacking, copying of software, introduction of viruses, unauthorised access or modification of computer material and other similar activities. The Act was amended by Part 5 of the Police and Justice Act 2006 to strengthen the legislation around unauthorised access and penalties for helping others to commit computer misuse.

Regulation of Investigatory Powers Act 2000 (RIPA)
RIPA 2000, and The Telecommunications (Lawful Business Practice) Regulations 2000, provides a framework for monitoring activity, data and persons to assist in the detection and prevention of crime in relation to the Council's work. Interception of data or communications must be relevant, necessary and proportionate

Copyright, Designs and Patent Act 1988
This legislation gives the creators of materials and information rights to control the ways in which their materials may be used.

The legislation places restrictions on the copying and use of copyright material including computer software, publications and images and as such unauthorised copies of information, documentation or software may not be made.

.

APPENDIX B

RECORDS MANAGEMENT – LEGISLATION & STANDARDS

Local Government Act 1972
Section 224 of the Act requires local authorities to make proper arrangements in respect of the records they create.

Public Records Acts of 1958 and 1967
All public bodies have a statutory obligation to keep records in accordance with the Public Records Act. This places the responsibility on government departments and other organisations within the scope of the Act for making arrangements for selecting those of their records, which ought to be permanently preserved, and for keeping them in proper conditions. Parts of this Act have been superseded, partly by the FOIA 2000.

Limitation Act 1980
Has particular relevance to applying appropriate retention periods. For example, with regard to financial records, the Act "provides that an action to recover any sum recoverable by any enactment shall not be brought after the expiration of six years from the date on which the cause of the action accrued".

Health and Safety at Work Act 1974
Influences how long records relating to Health and Safety incidents should be retained.

International standard for records management: ISO 15489.
Aims to ensure that appropriate attention and protection is given to all records, and that the evidence and information they contain can be retrieved more efficiently and effectively, using standard practices and procedures.

Code of practice for information security management: ISO 17799
ISO 17799 describes a structured set of control objectives, the implementation of which is guided by an assessment of information security risks. It also proposes a governance framework for the management and implementation of information security.

Information Security Management System requirements: ISO 27001
This is complementary to ISO 17799 and defines the requirements for an Information Security Management System (ISMS). This, effectively, describes the process for creating an ISMS, implementing and managing the governance and controls described in ISO 17799.

Code of practice for Legal Admissibility: BIP 0008
Provides a framework and code of good practice for the implementation and operation of information storage systems, whether or not any information held therein is ever required as evidence in event of a dispute.

e-Government Interoperability Framework: e-GIF
e-GIF defines the technical policies and specifications governing information flows across government and the public sector. They cover interconnectivity, data integration, e-services access and content management.

e-Government Metadata Standard: e-GMS

e-GMS is a subset of the e-GIF and lays down the elements, refinements and encoding schemes to be used by government officers when creating metadata for their information resources or when designing search systems for information systems.

Local Government Classification Scheme - Information & Records Management Society of Great Britain
This scheme seeks to achieve control over both electronic and physical records by ensuring that records, whatever their medium, are stored consistently. It aims to achieve this by ensuring that records be logically stored together in a functional structure and thereby "facilitate and enhance the capacity of the organisation to use and share information".

Retention Guidelines for Local Authorities – Information & Records Management Society of Great Britain
Guidance for local authorities on the retention and disposal of common functional and housekeeping records. To be used as a baseline to interpret and apply appropriately in accordance with local practice.

Building Systems Fit for Audit: BSI PD 0018
To ensure that IT information systems can be easily audited.

Lord Chancellor's Code of Practice on the Management of Records, Issued under section 46 of the FOIA
This Code of Practice gives guidance on good practice in records management, particularly in relation to the Freedom of Information Act.

The National Archives' (TNA) Requirements for Electronic Records Management Systems
Requirements used by TNA's system evaluation programme. Many of the leading IT systems are formally assessed and approved against these requirements.

Model Requirements for the Management of Electronic Records: MoReq
Requirements specifications funded by the European Commission. The second version of these requirements, MOREQ2, are set to supersede the TNA requirements as being the principal standard by which such systems are judged.

HM Government, Information Principles: December 2011

Generally Accepted Recordkeeping Principles, Information Governance Maturity Model: ARMA International 2013