BRENTWOOD BOROUGH COUNCIL

Information Security Policy

Title:	Information Security Policy
Purpose:	To ensure information is kept secure
Owner:	Data Protection Officer
Approved by:	Head of Legal Services
Date:	
Version No:	2.0
Status:	APPROVED BY PP&R COMMITTEE
Review Frequency:	Annually or when changes made to relevant Information Governance law
Next review date:	As above
Meta Compliance	IT to ensure policy subject to this

1. Introduction

This policy defines the Information Security Policy and is part of the Information Governance suite of policies including:

Access Control Policy

E Mail Policy

Information Classification & Handling Policy

Physical Security Policy

Conditions of Acceptable Use

Corporate Information Security Policy

.

2. Context

Information is essential to delivering services to our customers and the businesses we work with. Information security refers to the protection of physical information or information systems from unauthorised or unintended access, destruction or tampering. It is important to act appropriately with the information we hold. Confidentiality, integrity and availability of information must be proportionate to maintain services, comply with the law and provide trust to our customers and partners. Consequences of unauthorised access/loss of information, in particular personal data, can result in serious financial and reputational harm to BBC, its customers and businesses.

3. Application of Policy

Everyone who accesses information we hold must be aware of these policy statements and their responsibilities in relation to information security.

The Council commits to informing its employees, members, voluntary workers, agency staff, contractors and other third parties of their obligations before they are authorised to access systems and information and subsequently at regular intervals. Other organisations and their users granted access to information held by our organisation must abide by this policy.

All those who access information may be held personally responsible for any breach or misuse.

4. The law

Article 32 of the GDPR says:

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    1. the pseudonymisation and encryption of personal data;

    2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

    4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

OBLIGATIONS

- Only access systems and information for which you are authorised.
- Only use systems and information for the purposes authorised.
- Comply with all applicable legislation and regulation.
- Comply with controls communicated by the Council, its Service Managers ('Information Asset Owners') and the Data Protection Officer (DPO).
- Do not disclose confidential or sensitive information to anyone without the permission of the Council. In practice, this will usually be your line manager but if in any doubt, please contact the DPO for guidance.

- Ensure confidential or sensitive information is protected from view by unauthorised individuals. See our **Clear Desk Policy**
- Do not copy, transmit or store information to devices or locations (physical or digital) where unauthorised individuals may gain access to it; the security of devices and locations you use are your responsibility.
- Protect information from unauthorised access, disclosure, modification, destruction or interference.
- Keep passwords secret and do not allow anyone else to use your access to systems and accounts.
- Notify the DPO of any actual or suspected breach of information security and assist with prompt resolution, including taking all steps necessary to limit breaches and to avoid repetition of such breaches.
- Co-operate with compliance, monitoring, investigatory or audit activities in relation to information.
- Ensure you/your staff have completed the **online FOI and DPA awareness training.**

ROLES AND RESPONSIBILITIES

The organisation

- Ensures compliance with law governing the processing and use of information.

The Chief Executive

- Acts as the 'Accountable Officer' ensuring that all information is appropriately protected.

Senior Information Risk Officer

- Assures information security within the organisation
- Promotes information security at executive management level
- Provides and annual statement about the security of information assets

Data Protection Officer

- Manages the investigation and mitigation of information breaches
- Supports Management in assessing risks and implementing controls
- Keeps the SIRO fully briefed on all information risk matters

Service Managers (Information Asset Owners)

- Assess the risks to the information they are responsible for
- Define the protection measures of the information they are responsible for, taking account of the sensitivity and value of the information.
- Communicate the protection controls to authorised users and ensure controls are followed

- Ensure their staff have undertaken appropriate information governance training, including **online FOI and DPA awareness training.**

Senior Management Team

- Ensure their employees are fully conversant with this policy and all associated standards, procedures, guidelines and relevant legislation and are aware of the consequences of non-compliance.
- Introduce training and develop procedures, processes and practices which enable compliance with this policy across their business areas.
- Ensure all contractors and other third parties to which this policy may apply are aware of their obligation to comply with it.

Employees

- Conduct their business in accordance with this policy
- Take responsibility for familiarising themselves with this policy and understanding the obligations it places on them, with particular emphasis on the need to ensure no information is released, published or otherwise disclosed without prior authorisation from their manager.
- Ensure they have received appropriate level FOI/DPA training based on their level of access to information.

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you. The Council as well as those individuals affected is also at risk of financial and reputational harm. Fines of up to €20,000,000 may be imposed on Councils for serious data breaches. Please report any actual or potential data breaches or other concerns relating to Information Governance to the Data Protection Officer as soon as possible.

END OF DRAFT POLICY