Information Security Policy Statement

Version: 2.01

Version Awareness:

Please note that documents printed or downloaded are uncontrolled documents and therefore may not be the latest version.
Those within the scope of this document are responsible for familiarising themselves periodically with the latest version.

Title:	Bristol City Council Information Security Policy Statement		
Description:	This policy statement applies to the processing of BCC information (regardless of format) and/or the use of BCC provided ICT assets, infrastructure and services		
Manager Approver	Information Security Manager	**HoD Approver**	Head of Information Assurance
Author:	Information Security Officer	**Scope:**	All members of staff, visitors or third-party providers of services or support.
Document Status:	In Circulation	**Version:**	2.01
Classification:	Official		
Create Date:	07/06/2018		
Approval Body:	Information Governance Board	**Date Approved:**	25/11/2021
Document Review Period:	6 months from approval and annually thereafter unless a significant change is required.	**Disposal Period:**	Permanent

Document History

Version	Date	Editor	Details
1.00	07/06/2018	Information Security Manager	First draft.
1.01	19/07/2018	Information Security Manager	Minor edits following review.
1.02	14/10/2021	Information Security Officer	Template editing/reformatting.
2.01	25/11/2021	Information Security Officer	Signed off.

Contents

1. Policy Statement

1.1. Bristol City Council (BCC) recognises information as an important asset of significant value to the organisation. It also recognises the need to protect information and to ensure it is processed in a secure manner. This will be achieved by:

1.1. Confidentiality, Integrity, and Availability are the established basic principles providing the fundamental organisational principles that allow the management of information security:

- **Availability** is the ability of a system to ensure that access is not denied to any authorised party
- **Integrity** is the ability of a system to ensure that system is modified only be authorised parties
- **Confidentiality** is the ability of a system to ensure that an asset is viewed only by authorised parties.

1.1.1. Ensuring the confidentiality, integrity and availability of information and information assets belonging to BCC and entrusted to us by members of the public, our strategic partners and other third-party organisations.

1.1.2. Adopting and maintaining an Information Security Management System (ISMS) which considers comprehensive security controls aligned to ISO/IEC 27001:2013.

1.1.3. Continually improving the ISMS by measuring the effectiveness of controls and adapting to new and emerging risks.

1.1.4. Maintaining compliance with relevant UK and European Union legislation e.g. The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).

1.1.5. Establishing information security objectives to improve information security compliance.

1.1.6. Ensuring effective policies, standards, procedures and guidance are in place to support secure working practices.

1.1.7. Educating and training staff to handle and process information securely.

1.1.8. Ensuring specialist staff are available to provide support and guidance.

1.1.9. Investigating and reporting of all actual and suspected security incidents.

2. Scope

2.1. The Council's ISMS is applicable to information produced, handled and stored including hardcopy data, electronic data, Council records, policies and procedures, software and licenses and physical IT hardware from any source that is accessed by the Council.

2.2. The Information Security Management System boundary contains the logical and physical services, products and activities provided from their premises at its core locations.

3. Impact of Failing to Safeguard Information

3.1. BCC accepts that failing to safeguard information can have varying degrees of impact depending on the type of failure and the information involved. It includes:

3.1.1. Undermining of public confidence in public services
3.1.2. Negative impact in public finances
3.1.3. Embarrassment or distress caused to service users
3.1.4. Reduced effectiveness in the performance of business activities
3.1.5. Failure in the provision of local services
3.1.6. Wider reputational damage

4. Supporting Policies

4.1. This policy statement is supported by policy, standards and procedures.

4.2. The policies support a layered approach to protecting information and information assets. Layered approach refers to the application of different security controls rather than relying on a single control. This is often referred to as 'defence in depth' and more stringently 'a zero-trust model'.

4.3. In addition, BCC will ensure it provides and maintains an appropriate policy set designed to support appropriate information processing, for example a Data Protection Policy and Records Retention Schedule.

5. Compliance

5.1. BCC employees have a contractual responsibility to be aware of and conform to BCC's values, rules, policies and procedures. Breaches of policy may lead to the employee going through the Council's disciplinary procedure in accordance with the Code of Conduct and the Council's disciplinary policy and procedure.

5.2. Individuals who are not BCC employees and who fail to comply with BCC policies may have their access to Council information and ICT revoked and such action could have an impact on contracts with third party organisations.

5.3. Breaches of policy may lead to civil or criminal proceedings depending on the breach.