Working together

Bournemouth Borough Council & Borough of Poole Information Security Policy

1. Why do we have this policy?

Reason

Bournemouth Borough Council and Borough of Poole recognise 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)
- Counter-Terrorism and Security Act 2015
- 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 security of Information is essential to good government and public confidence. It is important that customers and organisations are able to trust the Council's to obtain, use and share their information securely and responsibly.

Both Councils will protect its information from threats that could disrupt the Council's work or infringe the rights of staff or its customers.

Purpose

The purpose of this policy is to set out the rules which help protect the Council's information and the information it holds about its customers (individuals, businesses and organisations), the public and staff. The policy helps prevent and reduce the impact of security incidents and consequently minimises the damage that may be caused to customers, the Councils and its assets.

Good information security is built on three basic components:
Confidentiality: Keeping information out of the wrong hands
Integrity: Making sure that information is accurate and complete
Availability: Ensuring the reliable and timely availability of information and services

This Information Security Policy provides the framework to ensure that:

- Information owned or processed by the Council is protected against threats, be they internal or external, deliberate or accidental.
- Confidentiality of information is assured – we will protect information being used by the Council from unauthorised access, use, disclosure or interception.
- Integrity of information is maintained – we will protect information from unauthorised changes or misuse, so that it can be relied upon as accurate and complete.
- Availability – information is available when and where it is needed.
- Legal, regulatory and mandatory compliance requirements are understood and met.
- Information and training on information security is up to date and is mandatory for all staff.

2. Who must comply with the policy?

All staff, contractors, partners and elected members must comply with this policy.

All users of the Council's IT systems and information must observe the requirements of this policy when accessing and/or using the Council's information, information systems, software or hardware.

Staff are responsible for ensuring others working on their behalf (e.g. temporary staff, contractors, partners, etc.) are aware of and abide by this policy when undertaking Council business.

Access to some systems will require users to read and sign additional declarations.

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

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

4. What is this policy?

Approach

This Policy is based on industry guidance and on aspects of ISO 27001:2013; "Information Security Management Systems – Requirements" and related guidance.

The Councils are also required to adhere to Government's Public Services Network (PSN) security standards and the Payment Card Industry Data Security Standard in order to provide services and process payments.

The Councils recognise the need to match the implementation of the Information Security Policy to the security risk and the impact of a security incident or breach. The policy aims to establish a fair balance between security requirements and the expectations of the Councils and users. However, there should be no expectation of privacy amongst any user who uses or accesses the Council's IT infrastructure or email service to create, store, send or receive information.

Breaches of this Policy
Breaches of this policy must be reported to immediate line managers at the earliest opportunity.

Information Security Policy – Guidance
The policy guidance explains the aspects of security all users are responsible for and what they must do to maintain good security and ensure they are working within the policy. There are also separate technical controls documented and held by ICT Services within the Councils. Guidance can be found on the Information Governance and ICT pages on the Council's intranet pages.
The guidance will enable the Council to:-

- Manage and provide direction and support for information security.
- Provide a clear hierarchy and procedures for reporting, monitoring and decision-making that adheres to relevant legislation and policy.
- Minimise and/or mitigate the risk of the authority being brought into disrepute or becoming liable to prosecution for breach of legislation, accepted working practices, or general employer responsibility.
- Define and schedule activities to test the effectiveness and application of this Policy.

General Requirements

- The effectiveness of this policy will be checked by regular internal audits.

Information Security Incident/Breach Reporting and Liability

- If a security incident or breach is suspected the matter must be reported to the responsible line manager, the Information Asset Advisor, the Information Governance Team and (where IT hardware or IT systems are involved) the ICT Service Desk immediately for advice and guidance. If the incident or breach relates to social care information the Caldicott Guardian must also be informed. Information connected with the incident or breach must not be changed or added to.
- In the event of an act that exposes the Council to risk of corporate liability and/or prosecution the matter may be treated as a disciplinary offence, which could in some cases lead to suspension/termination of employment and/or the Councils or another prosecuting body taking legal action against the individual concerned.

Monitoring and Restrictions
The forms of network, user and data monitoring used by the Councils are described below:

- Incoming and outgoing emails and attachments are captured and retained within the email archive software for at least 2 years.
- Filtering software is used to block access to websites deemed by the Councils to be inappropriate. Websites deemed to be inappropriate will be regularly reviewed and updated.
- Emails and attachments are electronically scanned for inappropriate content, viruses & malicious code. Emails trapped and quarantined can be checked by IT or the Information Governance Team. If a policy breach is suspected the relevant Service Director/Head of Service will be informed, who may initiate further action.
- Service Directors/Heads of Service may approve the supplementation of regular electronic monitoring if it is believed that a breach of this policy is being or has been committed. This may include, but is not restricted to, accessing the content of

emails, telephone logs and website logs. Users will be informed if such directed monitoring takes place.

- If covert investigations are deemed necessary, because criminal activity is suspected, the Regulation of Investigatory Powers Act (RIPA) requirements will be met. Monitoring of this type will only take place with the approval of the Council's authorising officer, or the Managing Director/Chief Executive.
- Staff involved in testing this policy, security related monitoring, reporting the analysis of findings or disciplinary proceedings relating to information security must be aware of, and abide by, relevant Council policy and legislation; they must also respect confidentiality.

Communications Security

The Councils will ensure that users are provided with the information they need to communicate and use information in ways that:-

- Prevent the loss, modification or misuse of information between users and organisations.
- Minimise the risk of harm or offence due to inappropriate material.
- Enables them to take all possible care of the information they receive, use or produce.

Using or Exchanging Information (e.g. email, Internet, telephone, letter)

- Users must observe any specific Councils guidance developed for the exchange or transmission of information, including email guidance, PSN compliance or PCIDSS compliance for payment data.
- Users must observe any Councils policy and guidance covering the use of Social Media.
- Information must only be disclosed to, or exchanged with people or organisations that are entitled to have that information. If users are unsure advice must be sought from relevant line managers, Information Asset Advisors, or the Information Governance Team.
- When users use their own device(s) to access the Council's IT hardware/software, they must adhere to this policy.
- The risk associated with exchanging information should be assessed and appropriate mitigating actions taken, e.g. encryption or secure email.
- Special category data (sensitive), personal or confidential information must only be exchanged where desensitised or anonymised information is not sufficient and is in accordance with the Data Protection Act.
- Users transmitting or sending personal or confidential data off site must use a secure method, which includes secure GCSX email, encrypted email or encryption if on physical media. The Council's normal email system is sufficient to send personal data off site, including sending to other public sector bodies.
- Email or any other method of communication must not be used to commit the Councils to a course of action you are not authorised to take, e.g. enter into a contract or distribute confidential data.
- Personal email or social media accounts must not be used to do the Councils business.
- Users may use the Council's email and Internet system for reasonable and "appropriate" non-work related use. Councils email accounts must not be used to register on non-work related websites.

- Users must not use Councils equipment, accounts or work time to try to access, download, store, send or distribute material that can be construed as inappropriate or take part in inappropriate activities.
- If users receive or accidentally access inappropriate material they must exit it immediately and inform their Line Manager and the ICT Service Desk.

Inappropriate content and activities includes:-

- Pornographic material e.g. nakedness, sexual behaviour or sexual language.
- Discriminatory or defamatory content on the grounds of race, gender, sexuality, disability, sexual orientation, religion, age or any other characteristic covered by Equalities Legislation.
- Hateful, inciting, libellous, bullying, violent or abusive content including swearing.
- Extremist or radical content as defined in the Counter-Terrorism and Security Act 2015 and the Prevent Duty Guidance (see Appendix B).
- Participating in or encouraging any illegal activity e.g. hacking.
- Wasting work time e.g. gaming, gambling, chain mail, trading or the personal use of on-line chat, social media and networking websites.
- Divulging secure, sensitive or potentially damaging Council information, particularly via participation in "chat" rooms or "blogs", accidentally or on purpose.
- Developing, downloading, installing or storing unauthorised software, freeware, shareware or websites or non-work related pictures, music or video.
- That which would breach the Council's Employee or Member Code of Conduct.

This list is not exhaustive and the Council reserves the right to determine other materials or activities which are against the rules and spirit of this or other Council policies. If such materials or activities are identified, they will be communicated to users.

Access Control

The Councils will control access to information, applications, systems and resources to help prevent unauthorised access. It will provide information for users, through this policy and other measures, to ensure they know their responsibilities and the importance of good information security.

Access to systems – New starters, leavers and changes

- Access for users to use any system must be formally requested by the responsible manager or Information Asset Owner, using the 'New Starter' form or by contacting the Service Desk.
- Only the appropriate, minimum level(s) of access needed by users to do their jobs should be requested.
- Only a manager or Information Asset Owner can request changes to access levels or additional access.
- Managers must ensure that users' access rights are reviewed regularly. This is of particular importance where users are changing roles, leaving or have been suspended from duties.
- Access rights that allow users to carry out tasks that would usually not be permitted by other regulations will normally not be granted, e.g. the same user raising and approving a purchase order. Where such access is required on a "by exception" basis Service Director/Head of Service approval is required.
- Managers must inform IT in advance of users leaving, with advice on the retention of any data and who should be given access to it.

- Where there is a specific and pressing business need to access information, such as that held in a person's email account, on a personal drive or in a system, this access must be formally requested via the IT Service Desk and approved by the responsible manager.

Password Standard

The Councils have a defined password standard, which it enforces where technically possible. It is based on industry good practice and Government security requirements.

The Councils password standard is:

- A minimum of 9 characters
- Must contain 1 capital letter
- Must contain 1 numeric value
- Must not be any of a user's previous 3 passwords
- Must not contain a user's full name or username
- Must be changed every 90 days

- Passwords will be changed the first time new staff log on to the Councils network.
- Users must change their password if it has been compromised or they believe someone else knows what it is.
- Passwords must be kept secret, not written down or shared
- In applications where the password standard cannot be automatically applied users will apply the Council's password standard, as far as possible.

Locking Workstations

- Users must "lock" their computer screen when they are leaving it unattended for any period of time. Users must not leave screens showing confidential or special category information. This is particularly important in public areas or where personal or financial information is used.

Remote and Mobile Access

- Technological solutions, over and above user ID and password authentication, will be implemented where possible and it is felt that the sensitivity and confidentiality of the information or the method of access requires heightened control or where hardware may become unsecured.
- The loss or theft of Councils information or a device which may hold information (e.g. laptop or mobile device (including your personal device if you have access the Council's IT hardware/software) must be reported to the ICT Service Desk, the Information Asset Advisor and the Information Governance Team as promptly as possible.

Operations Security

The Councils will protect the integrity of the information and systems it uses to prevent the loss or corruption of information or the failure of computer systems. The Councils have measures in place which act to counteract interruptions to business activities and to protect critical business processes from the effects of major failures and disasters.

Malware & Virus Protection and Prevention

- If users become aware of a potential information security weakness or threat such as a virus they must report it to the IT Service Desk and follow any instructions they provide
- Users must not open suspicious emails, email attachments, Internet links or "pop-up" programmes, particularly if they come from an unknown sender or are executable files (end with .exe, vb, scr). Report to mailabuse@bournemouth.gov.uk
- If a virus is suspected or detected IT may isolate a computer, equipment and any potentially infected media.
- All CD, DVD, USB devices are scanned automatically for malware and viruses by IT; any attempt to deliberately infect a Council system may lead to disciplinary proceedings.
- If staff are concerned or doubtful about information they receive or access they should seek guidance from the IT Service Desk.

Printing & Information Storage and Disposal

- Users must be aware of the legislative constraints (DPA) when they print special category information; ensuring printouts are not left on display or unattended.
- Users must dispose of special category information or confidential documents using the Council's confidential waste bins (see Appendix A for definitions)
- Media such as hard drives including removable drives, tapes, CDs or DVDs, data cards and USB sticks must be destroyed by ICT Services.

Operations and Network Monitoring

- Users are encouraged and expected to report abnormal, unusual or unacceptable network or application performance to the ICT Service Desk for investigation.

Information Security Continuity

- ICT Disaster Recovery arrangements are tested annually and will be reviewed and updated as areas of business risk are identified and Business Continuity arrangements are developed.
- Managers must liaise with ICT Services to validate the IS/IT elements of their Business Continuity plan

Human Resources Security

All users have a crucial role in good information security. The Councils will ensure users are aware of their responsibilities and trained to use information and systems appropriately and securely to help reduce the risk of human error, theft, fraud or misuse. The Councils will ensure appropriate checks are done prior to users having access to the Council's systems and information.

Recruitment

- Managers must consider whether security responsibilities, over and above those generally required, need to be included in job descriptions or contracts due to the nature of the duties involved.
- Managers must liaise with HR and ensure any relevant vetting or checking is completed before users are given access to information or systems or when users change roles.

Training and awareness

- Users will be provided with information on security and given the opportunity to receive training.

- Managers and supervisors must ensure users are adequately trained to use the information systems they need to use in a safe and secure manner.
- Managers must identify and address information security training requirements for users on the basis of their job functions and the computer systems/information they are required to access.

Termination or Change of Employment

- Managers must consider and act on the security aspects of a user leaving, changing role or subject to suspension.
- Users must uphold their obligations towards information security under privacy laws and contractual terms.

Physical Security

The Councils will ensure it has measures in place to prevent unauthorised access, damage and interference to information, hardware and premises. Users will be made aware of their responsibilities in preventing the loss, damage or compromise of information or hardware.

Physical Access Control

- Users should not try to gain access to areas they are not permitted to enter or have no need to enter.
- Users must help maintain good security by not allowing the public or visitors into areas they are not authorised to be in and by challenging people who are in an area they shouldn't be.
- Access controlled doors must not be left open unattended. Any lost swipe cards must be reported immediately.

Remote Working

- Managers should ensure security risks are assessed and necessary adjustments made to protect Councils equipment and information used by home or remote workers.
- Users must take all reasonable steps to ensure that mobile/portable information storage devices (laptop, tablet, USB sticks, mobile phones, etc.) are not placed at risk of loss, theft, or damage. Devices must be kept securely at all times, which includes while in transit, at home or in any other off-site location.
- Authorised users must take all appropriate measures to ensure that information and hardware is not accessed or used by unauthorised people or used for unauthorised purposes.

Asset Management

The Councils will ensure that its information and physical assets are managed effectively and receive the appropriate level of protection.

Hardware and Software Inventory Management

- No computer or network communications hardware should be moved without the agreement of ICT.
- No computer, network communications hardware or software should be taken off Councils premises without prior senior line management and ICT agreement.

- Users must only use hardware owned by the Councils or approved by ICT to connect to the Council's network or for Council business. If you are using your own device to access the Council's IT hardware/software you must adhere to this policy.
- Users must only use hardware or methods of connection that are owned by the Council or approved by ICT to connect to the Council's network or for Council business.
- Software and hardware used on the Council's network or computer equipment must be installed by ICT or with their approval / assistance.
- Computer hardware and software must only be disposed of by ICT.

Information Storage

- Users will store and retain data as defined in their Service Unit's Retention and Destruction Schedule.
- Managers will have arrangements in place that provide relevant users with access to other users' business information where this is required to ensure service delivery in the event of planned or unplanned absences. Such arrangements must also take account of managing the receipt of requests for information under the FOIA/EIRs/DPA.
- Council Information must be saved in the appropriate team folder in the Shared Drive or within the appropriate business area case management tool. You must avoid storing information on hardware e.g. laptop, mobile phone or tablet as this will not be backed up by the Councils.
- Unattended desks/workstations must be cleared of special category/confidential information

Systems development and maintenance

The Councils will ensure that security management is built into its systems and processes in order to protect the confidentiality, authenticity and integrity of information and applications.

Hardware, Software and Systems

- Users must follow the Council's processes for the justification and purchase of hardware, software and systems, in order to ensure compatibility and adequate security controls.
- Users must not attempt to, or actually, obtain unauthorised access to or tamper with or change hardware, information or software applications used /owned by the Councils.
- Users must not copy software, except as allowed under its licence and with the permission of ICT.

Change Management

- Changes and upgrades to systems must only be done by or in consultation with ICT Services to minimise the risk of problems and adverse impact on services.
- Changes must be planned and carried out in conjunction with the appropriate Service Unit(s) and signed off by them.
- Minor changes (new software, moving hardware etc.) must be requested via the ICT Service Desk.

Compliance – Legislation and Council Policy
Some aspects of information security management are supported by legislation (see Appendix B). Users must make themselves aware of the legislation and abide by it in order to avoid breaches of criminal and civil law and statutory, regulatory or contractual obligations.

- The Councils will have nominated staff, Information Asset Advisors within all of its Service Units to provide information security advice.
- The Information Governance Team and the ICT Team will provide more detailed and specific advice to staff, councillors and the Councils on all matters relating to information security.
- Basic information security 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.
- Information security 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.
- All councillors will undertake information security awareness training, delivered by the Information Governance Team.
- The Head of Information Governance (HoIG) can refer Service Units that are causing concern in respect of information security to the Information Governance Board and Audit & Governance (A&G) Committee
- The HoIG will report on the Council's information governance function to the Audit & Governance Committee at regular intervals, as agreed with the A&G Chair. This will include reporting on any breaches of information security, which have been reported to the Information Commissioner.
- The Councils will investigate information security incidents and breaches. Staff will be trained in reporting and managing information security incidents and breaches.
- If an information security breach meets the reporting criteria as set out by the Information Commissioner's Office, the Councils 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.

Complaints
We will adopt the Council's complaint procedure to acknowledge and resolve any complaints or issues.

Complaints relating to any alleged breach of information security should be made in writing and addressed to:

Complaints Manager
Bournemouth Borough Council
Town Hall
Bourne Avenue
Bournemouth
BH2 6LL

Or

Complaints Manager

Borough of Poole
Civic Centre
Poole
BH15 2RU

The Councils will respond appropriately to any complaints referred to it by the ICO.

Data Protection Officer
The Councils' Data Protection Officer, in accordance with the requirements of the GDPR/DPA 2018, is the Head of Information Governance and can be contacted at: information.governance@bournemouth.gov.uk.

5. How is this policy implemented?

Through staff procedures, processes and guidance which are published to the IG and ICT pages of the Council's intranet service, e-learning packages and the delivery of training by the IG Team.

Procedures, guidance and training

Procedures, guidance and details of IG training services are available on Biz and The Loop

Roles and responsibilities
The **Managing Director/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 securing information in their ownership, they may appoint Information Asset Managers to assist them with these duties.

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

Data Protection Officer is responsible for giving independent advice on Data Protection legislation and reporting to senior management about compliance with the law.

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.

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 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 legislation and the wider information governance function, which includes the Data Protection Act and relevant legislation.

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

Enforcement
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.org.uk

Effective from date	July 2018
Review date	July 2020
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 The Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 Common law Duty of Confidentiality Privacy and Electronic Communications Regulations 2003 General Data Protection Regulations 2016
Related policies	Information Governance 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)	BBC	
Corporate Policy & Strategy Officer	BBC	
Information Asset Advisors	BBC	
Head of ICT	BBC	
Head of Strategic HR	BBC	
Senior Information Risk Owner & Deputy SIRO	BBC	
Caldicott Guardian	BBC	

Head of Audit & Management Assurance	BBC	
Equality & Diversity Managers	BBC	
Consultation & Market Research Manager	BBC	

Equality Impact Needs Assessment

Assessment date	

Freedom of Information Act Exemption

FOI Exempt?	**NO**

Appendix A

Definitions and terms

The following terms are included to help with the understanding of this policy.

Information - Includes all manual or electronic information/data processed by the Councils

Software - Operating systems, applications, utility software, shareware etc.

Hardware - A physical device that can hold information or connect to the network.

User – Authorised persons with access to Council information who work for, with or on behalf of the Council, e.g. staff, contractors, partner agencies, agency staff, etc.

Manager – Section/Department manager and above

Supervisor - Staff whose job role makes them responsible for staff and their appraisals.

Information Asset Owner – Service Director or officer(s) to whom Service Directors have delegated information asset ownership management and responsibilities

Security Incident – Where personal or confidential data held by the Council has been placed at risk of disclosure to an unauthorised third party, but no breach has subsequently occurred.

Security Breach – Where personal or confidential data held by the Council has been disclosed to a third party (internally or externally) who is not authorised to receive the information.

Appendix B

Legislation relevant to information security

Human Rights Act (HRA) – 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 (DPA) & General Data Protection Regulations 2016 (GDPR)
The 2018 Act governs and regulates how personal information is used, replacing the 1998 Act of the same name. It incorporates the General Data Protection Regulations 2016. The Act defines six basic rules or principles, which the Council must adhere to. A breach of any of the principles is a breach of the law.

The Act requires the Council to take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing and against the accidental loss or destruction of, or damage to, personal information.

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
- trade union membership
- physical/mental health
- sexual life
- commission of offences
- proceedings for offences and sentences of Court

- genetic and biometric data
- location data including IP address

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. Bournemouth Borough 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.

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

Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations (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. The release of such information into the public domain by whatever means will represent a breach of information security.

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

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.

Counter-Terrorism and Security Act 2015
The Act contains a duty on specified public sector bodies, including councils, to have due regard to the need to prevent people from being drawn into terrorism. This is known as the Prevent Duty. The requirements of the Act are embodied in the Prevent Duty guidance.

Extremism is defined in the legislation as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and

tolerance of different faiths and beliefs; or calls for the death of members of UK armed forces, whether in this country or overseas.

Radicalisation is defined in the Act as material in support of the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

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.