Agenda Item No:	9
Report To:	Cabinet
Date:	14 July 2016
Report Title:	Data Protection Policy
Report Author:	Nicholas Clayton, Senior Policy, Performance and Scrutiny Officer Paul Courtine, Senior Solicitor (Strategic Development)
Portfolio Holder:	Callum Knowles, Portfolio Holder for Information, Technology and Communications

Summary:	Ashford Borough Council needs to collect and use certain information about service users to allow us to carry out our many and varied functions and responsibilities. This personal information - however it is acquired, held, processed, released or destroyed - must be dealt with fairly and lawfully. Similarly, the information stored and processed by the Council, or by third parties working on behalf of the authority, is an equally valuable asset. Without adequate levels of protection, confidentiality, integrity and availability of information, the Council will not be able to fulfil its obligations including the provision of government services and meeting legal, statutory and contractual requirements. Accordingly, The Council's Data Protection policy has been brought up to date to ensure that it aligns with national legislation and policy, best practice from around the county and across the council, and following a recent internal audit of the council's data protection arrangements.

Key Decision:	NO
Affected Wards:	All
Recommendations:	**The Cabinet be asked to recommend to Council:-**

i. The revised Data Protection Policy and withdraw the Information Security Policy

ii. Authorise the Director of Law and Governance to approve minor amendments to the policy in the line with working arrangements.

Policy Overview:	Alongside the Data Protection Act 1998, a list of statutory legislation which governs aspects of the Council's data protection and information security arrangements are contained within the policy.
Financial Implications:	None
Impact Assessment	Attached
Other Material Implications:	None
Background Papers:	N/A
Contacts:	nicholas.clayton@ashford.gov.uk – Tel: (01233 330208)

Agenda Item No. 9

Report Title: Data Protection Policy

Purpose of the Report

1. The overarching purpose of this policy is to ensure that the data which the council uses is both secure and dealt with according to the appropriate legislation.

2. The policy has been brought up to date to ensure that it aligns with national legislation and policy, best practice from around the county and across the council, and following a recent internal audit of the council's data protection arrangements.

Background

3. Ashford Borough Council needs to collect and use certain information about service users to allow us to carry out our many and varied functions and responsibilities. This personal information - however it is acquired, held, processed, released or destroyed - must be dealt with fairly and lawfully. The Council will work within the terms of the Data Protection Act 1998 ("the Act") in all its dealings with personal data.

4. Similarly, the information stored and processed by the Council, or by third parties working on behalf of the authority, is an equally valuable asset. Without adequate levels of protection, confidentiality, integrity and availability of information, the Council will not be able to fulfil its obligations including the provision of government services and meeting legal, statutory and contractual requirements.

5. Whilst good data security is often the product of common sense, it is important that the council puts in place appropriate safeguards and protections to ensure that information is used appropriately and is not left vulnerable to misappropriation or misuse.

6. Appropriate information security ensures business continuity and minimizes business damage by preventing and minimizing the impact of security incidents.

7. Historically, data protection and information security have formed two distinct policies. With the increasingly interconnected digital world, and the proliferation of more means of communication and data-sharing, it was considered the opportune time to streamline the Council's policies in these overlapping areas into one policy document.

The Policy

8. The Council regards the lawful treatment of personal information as central to our operations, and to maintaining the confidence of our users. The policy sets out the council's obligation to comply with the following Data Protection Principles in relation to personal data:

    a. will be processed fairly and lawfully and, in particular, will not be processed unless specific conditions are met ;
    b. shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
    c. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
    d. will be accurate and kept up to date;
    e. will not be kept for longer than is necessary;
    f. will be processed in accordance with the rights of the data subject;
    g. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
    h. will not be transferred to countries outside the European Economic Area unless special conditions are met.

9. Moreover, the policy also sets out the Council's commitment to information security and provides the guidelines and frameworks for ensuring all forms of information, supporting systems and networks are protected from security threats such as malicious software, unauthorised access, computer misuse, information technology failures, human error and physical security threats. This approach is led by a number of key principles:

    a. Information is protected against unauthorized access
    b. Confidentiality of information is assured
    c. Integrity of information is maintained
    d. Regulatory and legislative requirements are met
    e. Information security training and e-learning is available to all staff and elected members
    f. All breaches of information security, actual or suspected, are reported and investigated
    g. Business requirements for the availability of information and information systems will be met.

Equalities Impact Assessment

10. Attached (Appendix A)

Other Options Considered

11. There are no alternative options if the council is to deliver a robust policy framework for its data protection and information security. If Cabinet chooses not to approve this policy, there is potential for the local community and partners to view the council as having disregard for its responsibilities in these areas.

Consultation

12. The Data Protection Policy has been drawn up in concert with colleagues from the Council's IT, Legal, Personnel and Development and Policy Teams.

13. Following consideration by the Council's Management Team, the draft policy will also be considered by the Joint Consultative Committee. This ensures that staff and union representatives are made aware of any changes affecting staff.

14. Whilst data protection will no longer form part of staffs' terms of service, non-compliance against the policy may still constitute misconduct.

Conclusion

15. The Council is committed to preserving the confidentiality, integrity and availability of our information assets within the jurisdiction of the Council:

    a. For sound decision making
    b. To deliver quality services to our customers
    c. To comply with the law
    d. To meet the expectations of our customers and citizens
    e. To protect our reputation as a professional and trustworthy organisation
    f. To safeguard against fraudulent activity.

16. Robust data protection and information security processes work to compliment each other and ensure that the council is able to operate effectively and efficiently. With the recent internal audit noted above, it is a prescient opportunity for the organisation to update the Council's policy arrangements. An updated Data Protection Policy will ensure that the council is exercising fully its responsibilities in this important area.

17. The policy will be reviewed every three years, or sooner if there is a change in legislation or government guidance.

Portfolio Holder's Views

18. "Data protection is everyone's business, and I am pleased to see that the Council has acted on recent internal audit findings, and drawn from the latest thinking and best practice, to revise its policy response in this important area. Robust means of ensuring the council's own data security, the necessary protections for sensitive information relating to individuals, and good overall information management, is crucial for a modern public body. I commend the attached revised policy to Cabinet."

Contact: Nicholas Clayton, Policy and Performance Officer
Email: Nicholas.clayton@ashford.gov.uk

Appendix A: Impact Assessment

Appendix B: Ashford Borough Council Data Protection Policy

ASHFORD
BOROUGH COUNCIL

Impact Assessment

When is an assessment needed?

Councils must assess the impact of ***proposed policies or practices*** while they are being developed, with analysis available for members before a decision is made (i.e. at Cabinet).

Broadly, *policies and practices* can be understood to embrace a full range of different activities, such as Cabinet decisions which substantially change the way in which we do something, setting budgets, developing high-level strategies, and organisational practices such as internal restructuring. Assessments should especially be undertaken if the activity relates closely to an equalities group (see next page).

Importantly, this does not include reports that are 'for note' or do not propose substantial changes – assessments should only be considered when we propose to do something differently.

1. General Information	
1.1 Name of project, policy, procedure, practice or issue being assessed	Data Protection Policy
1.2 Service / Department	Legal & Democratic
1.3 Head of Service	Terry Mortimer
1.4 Assessment Lead Officer	Nick Clayton
1.5 Date of Assessment	01/07/2016
1.6 Is this assessment of an existing or a proposed project, policy, procedure, practice or issue?	Proposed revised pol icy

2. What is Being Assessed?	
2.1 What are the aims of this project, policy, procedure, practice or issue?	to ensure that the data which the council uses is both secure and dealt with according to the appropriate legislation.
2.2 Who is intended to benefit from this project, policy, procedure, practice or issue?	All staff and Elected Members by ensuring that they comply with all regulations and act appropriately with regard to data and personal information. Residents and service users, by ensuring robust processes for dealing with the information they provide to the council.
2.3 Who else is involved in the provision of this project, policy, procedure, practice or issue? i.e. other sections, public or private bodies	
- within Ashford BC	Policy and Performance, Information Technology, Personnel and Development, Joint Consultative Committee
- from other agencies	Information Commissioner's Office

3. Possible Sources of Information

In order to assess the impact of proposed decision it is important to bring together all information you have on it to, analyse them and come to conclusions on how it affects those with protected characteristics.

Information on a policy, project or procedure can come in many forms :-

□ Census and other demographic information
□ User satisfaction and other surveys
□ Previous consultation exercises
□ Performance Indicators
□ Eligibility Criteria
□ Service uptake data
□ Complaints
□ Customer Profiling
□ MOSAIC data

I order to come to conclusions on impacts in section 4 you **must** have taken in to account all appropriate information, and be able to provide this if necessary in support of the judgements you make.

Also, it is not enough to have broad information on service users – to meet equalities duties this information **must** be broken down – where applicable – into the relevant protected characteristics which may be affected by this decision. For example, when considering disabled access to a new community facility, overall usage figures are not enough – an understanding of how many disabled users within this total must be demonstrated.

The protected characteristics are :-

Age Disability Gender reassignment Marriage and civil partnership Pregnancy and maternity

Race Religion and belief Sex Sexual orientation

More information on the definitions of these characteristics can be found here - http://www.equalityhumanrights.com/advice-and-guidance/new-equality-act-guidance/protected-characteristics-definitions/

4. What judgements can we make?				
4.1 Does the evidence already available indicate that the project, policy, procedure, practice or issue may affect these groups differently? (please check the relevant box and provide evidence where possible	Positive Impact?	Negative Impact?	No Differential Impact	If yes, can it be justified (and how)?
Impact Factors:				
Age (please detail any specific groups considered)	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Disability (please detail any specific groups considered)	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Gender (please detail any specific groups considered)	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Gender Reassignment	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Marriage / Civil Partnership	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Pregnancy & Maternity	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Race (please detail any specific groups considered)	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Religion / Belief	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Sexual Orientation (please detail any specific groups considered)	☐	☐	☒	Policy relates to the use of information and personal details – as such it applies equally to all protected characteristics
Other (please specify)	☐	☐	☐	

5. Conclusions	
5.1 Does the decision maximise opportunities to promote equality and good inter-group relations? If "yes" please state how?	☒ Yes Secure, robust data forms the foundation of efficient and effective service delivery for all residents, regardless of their characteristics ☐ No
5.2 Based on the answers to the above can we confidently say that in its present form the decision treats different groups fairly (bearing in mind "fairly" may mean differently) and that no further amendment is required?	☒ Yes ☐ No
If further action is identified to ensure fair impacts please complete the Action Plan available on the intranet and attach it to this form	

6. Monitoring and Review	
How will monitoring of this policy, procedure or practice be reported (where appropriate)?	This policy, data protection arrangements and guidance will be reviewed every three years, unless there is a major change to the underlying regulations.
When is it proposed to next review the project, policy, procedure, practice or issue?	As above
Any additional comments?	None

Appendix B

Ashford Borough Council

DATA PROTECTION POLICY

Contents

Introduction and Policy Statement

1. Ashford Borough Council needs to collect and use certain information about individuals to allow us to carry out our many and varied functions and responsibilities - including the provision of government services and meeting legal, statutory and contractual requirements. This data is a valuable asset, and without adequate levels of protection, confidentiality, integrity and availability of information, the Council will not be able to fulfil these obligations whilst maintaining the confidence of service users.

2. Any personal information - however it is acquired, held, processed, released or destroyed - must be dealt with fairly and lawfully. The Council will work within the terms of the Data Protection Act 1998[1] ("the Act") in all its dealings with such personal data, and will also foster a wider culture of awareness of the Act, and its guiding *principles*, specifically that personal data:

    a) will be processed fairly and lawfully and, in particular, will not be processed unless specific conditions are met[2];
    b) shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
    c) shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
    d) will be accurate and kept up to date;
    e) will not be kept for longer than is necessary;
    f) will be processed in accordance with the rights of the data subject;
    g) appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
    h) will not be transferred to countries outside the European Economic Area unless special conditions are met.

3. The main rule is to be as careful with other people's personal information as we would expect others to be with ours. Good security is good practice and common sense.

4. The Council is also committed to preserving the confidentiality, integrity and availability of our information assets within the jurisdiction of the Council:

    - For sound decision making

[1] A copy of the Data Protection Act 1998 can be located at: http://www.legislation.gov.uk/ukpga/1998/29/contents

[2] In relation to this principle, the Council will also ensure the conditions are met as set out in schedule 2 of the Act for the processing of personal data and in schedule 3 of the Act for the processing of sensitive personal data

- To deliver quality services to our customers
- To comply with the law
- To meet the expectations of our customers and citizens
- To protect our reputation as a professional and trustworthy organisation
- To safeguard against fraudulent activity.

5. This policy therefore also sets out the Council's commitment to information security and provides the guidelines and frameworks for ensuring all forms of information, supporting systems and networks are protected from security threats such as malicious software, unauthorised access, computer misuse, information technology failures, human error and physical security threats. This approach is led by a number of key principles:

    - Information is protected against unauthorized access
    - Confidentiality of information is assured
    - Integrity of information is maintained
    - Regulatory and legislative requirements are met
    - Information security training and e-learning is available to all staff and elected members
    - Where appropriate, any serious breaches of information security, actual or suspected, are reported and investigated to see what lessons could be learnt. Examples might include the leaving of data storage devices in a public place
    - Business requirements for the availability of information and information systems will be met.

The Scope of this Document

6. The Council's information is in many forms including:
    - Hardcopy documents on paper and sent by fax
    - Electronic information stored on computers, remote servers, mobile devices, tapes, microfilm, CDs, external disks and USB portable storage devices
    - Verbal information (face to face conversations and over the telephone) – the general policy in this area would be that council business shouldn't be discussed in public

7. This policy therefore applies to all information assets held by the Council irrespective of their format and covers all locations into which Ashford Borough Council information is taken and/or accessed.

8. The policy provides an overview of the Act, outline the key principles, and provide an overview of the responsibilities of individuals.

9. This Policy applies to –

    - All staff and elected members
    - Contractors, agencies and partner organisations operating on behalf of the Council or on Council premises – incorporated as appropriate through the Council's procurement and / or contract procedures

10. The policy applies to all information used by the Council in conducting its work, and in relation to personal data any which is subject to the Data Protection Act 1998, including:

    - all personal data that is processed automatically;
    - any personal data held in a manual form in a relevant filing system;
    - any personal data held in an accessible record.

11. This policy is designed to protect the council, staff, clients, partner organisations and members of the public by preventing data protection breaches from happening. The policy seeks to ensure that personal data processed by or on behalf of the council is dealt with in full compliance with the Act.

Definitions

Data Protection Term	Definition
Data	Information that is, or is intended to be, processed by computer. The definition of data within the act also extends to information that is recorded as part of a relevant filing system.
Data Controller	Someone who determines the purposes for which and the manner in which any *personal*

	data are, or are to be, processed. This may be one person alone or jointly with other persons.
Data Processor	As defined in the Data Protection Act in relation to *personal data*, a "Data Processor" is any person (other than an employee of the *data controller*) who processes the *data* on behalf of the *data controller*.
Data Subject	The individual who is the subject of *personal data*, i.e. who the *personal data* is about.
Inaccurate Data	*Data* that is incorrect or misleading as to any matter of fact.
Personal Data	*Data* that relates to a living individual who can be identified from the data. The definition of "Personal Data" also extends to and includes opinions about the individual and any indications of intentions of any person in respect of the individual.
Processing	In relation to information or data, the Data Protection Act defines "processing" as obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the information or data. This could include: • Organisation, adaptation or alteration of the information or data; • Retrieval, consultation or use of the information or data; • Disclosure of the information or data by transmission, dissemination, or otherwise making available; and • Alignment, combination, blocking, erasure or destruction of the information or data
Sensitive Personal Data and Confidential Information	*Personal data* consisting of information about any of the following: • Racial or ethnic origin; • Political opinions; • Religious beliefs or other beliefs of a similar nature; • Trade union membership; • Physical or mental health or condition; • Sexual life; • The commission or alleged commission by the *data subject* of any offence; and • Any proceedings for any offence committed or alleged to have been committed by the *data subject*, the disposal of such proceedings or the sentence of any court in such proceedings. *Confidential information* may include – • Any commercially sensitive information,

	such as information relating to commercial proposals or current negotiations • Information relating to security, investigations and proceedings • Information provided in confidence

The Legislative Background

12. Alongside the Data Protection Act 1998, the following statutory legislation governs aspects of the Council's data protection and information security arrangements. This list is not exhaustive:

Legislation	Areas Covered
The Freedom of Information Act 2000	Public access to Council information
The Human Rights Act 1998	Right to privacy and confidentiality
The Electronic Communications Act 2000	Cryptography, electronic signatures
The Regulation of Investigatory Powers Act 2000	Hidden surveillance of staff
The Copyright Designs and Patents Act 1988	Software piracy, music downloads, theft of Council data
The Computer Misuse Act 1990	Hacking and unauthorised access
The Environmental Information Regulations 2004	Public access to Council information related to the environment
The Re-use of Public Sector Information Regulations 2005	The Council's ability to sell certain data sets for commercial gain

Our Policy Position

On the Principles of Data Protection

Handling and Collecting Information (Principles 1 and 2)

13. The Council will process all personal data for the purpose of providing an effective delivery of service in accordance with the aims, responsibilities and obligations of the Council.

14. All personal data will be processed in accordance with the Council's notification with the Information Commissioner. Under the Act, Data Controllers are required to notify the Information Commissioner of the processing which they under take. The Council will maintain its Data Protection Register entry. Heads of Service are responsible for informing the Data Protection Officer of any new purposes for which personal data are processed in order to ensure the Council's notification is kept up to date.

15. The Council carries out data-matching exercises to identify any anomalies or inconsistencies and also for the prevention and detection of fraud and when required by law.

16. All those accessing or processing personal data in connection with Council business are individually responsible for ensuring that they comply fully with the Act.

17. It is a criminal offence to knowingly or recklessly obtain or disclose personal data without the Council's consent, for example by using the data used at work for personal use. Staff should not process any personal data unless they are sure that they are authorised to do so.

Records Management (Principles 3, 4 and 5)

18. The Council will only collect personal data where there is a clear purpose for collecting and using the information.

19. The Council will not hold personal data for longer than is necessary.

20. All managers and staff will work towards ensuring that the personal data they hold is accurate and, where necessary, kept up to date.

21. Opinions recorded on a file must be carefully and professionally expressed.

Individuals' rights (Principle 6)

22. The Council will process personal data in line with an individual's legal rights.

23. The Council will ensure that any requests for access to personal data are handled courteously, promptly and appropriately. The Council will ensure that either the data subject or his/her authorised representative has a legitimate right to access under the Act, that the request is valid and that the personal data is communicated in an intelligible form. Guidance is available to staff on the intranet.

24. Detailed guidelines on dealing with data subject access requests will be made available on the intranet. Each service area has responsibility for providing the response to requests for access to personal information held by them, subject to any guidance from the Data Protection Officer.

Security (Principle 7)

25. All managers and staff are responsible for ensuring that personal data is held securely at all times, for example by locking their computer when away from the desk, and by keeping any personal data out of plain sight.

26. Paper files and manual records containing personal data must be kept secure both within and outside Council premises.

27. Access to all Council systems will be password protected and only authorised personnel will have access.

28. When working off site, Council employees are responsible for ensuring that personal data is held securely.

29. Records will be safely and responsibly disposed of when they are no longer required, for example by placing any paper copies in the confidential bins provided.

30. Data processing by a data processor must be carried out under a written contract and include specific obligations on the data processor. See the intranet for more information.

Transfer of Data (Principle 8)

31. Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA).

On related matters of Information Security

Email, Instant Messaging and Social Media

32. Email has quickly become an essential tool for conducting day to day business.

33. All emails that are used to conduct or support official Ashford Borough Council business should be sent using a "@ashford.gov.uk" address, Government secure GCSx email (when told to do so by the person you are in correspondence with) or another which has been agreed with the Council IT team. Other non-work email accounts should not be used to conduct or support official Ashford Borough Council business. Elected Members have a duty to comply with data protection principles, and the requirements of this policy. The advice from government is that the use of an @Ashford.gov.uk email address helps to achieve this.

34. Staff must not open attachments or click on hyperlinks within e-mails from unknown sources, and Councillors and staff must ensure that any emails containing sensitive information is sent from a recognised and agreed Council email.

35. The official Council disclaimer is automatically added to all emails sent to external addresses – this is an important security feature and should not be altered.

36. When forwarding or replying to a message, consider the chain of messages that precede it and whether these need to be sent on.

37. It is equally important to not divulge sensitive or confidential information through other electronic mediums – namely instant messaging and social media platforms. Details of the specific considerations to be made regarding social media can be found In the Council's social media policy.

Home and off-site working

38. Any laptop or other device that is taken off Council premises must be encrypted and allocated to the user.

39. All necessary precautions must be taken to ensure the security of hard copy documents that are taken off Council premises.

40. All home working and remote working must be carried out in compliance with relevant policies and procedures and have the authorisation of the relevant line manager. Please see the Council's *Home Working policy* for further details.

41. Council staff working off-site with Council-owned personal data must ensure that they abide by the provisions of the Act. In particular, Council-owned data which taken off-site for home-working must be transferred and held securely, not transferred to a third party and must be used only for official Council business. Personal data should not be retained on home computers beyond the time needed for the home work to be completed.

42. As such, personal data relating to Council customers, clients, employees, members or third parties such as suppliers or contractors must not be removed from Council offices by staff without the express authorisation of the appropriate manager. When Council-owned data is away from the Council offices, staff are solely responsible for the security of the data and must take reasonable precautions to prevent unauthorised persons gaining access to it. This may include not leaving storage devices or computers unattended in public spaces, or ensuring that such devices are password protected.

Disposals

43. Staff must ensure compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive and ensure that sensitive data is not accidentally released. The disposal of any IT and associated equipment must be carried out by ICT.

44. Sensitive and confidential information should be disposed via the confidential bins provided.

45. If working at home staff must comply with the above disposal methods which ensure secure methods such as shredding. If no secure disposals methods are available, sensitive information must be transported to your normal working area for secure disposal.

46. It is important to keep the waste in a secure place until it can be collected for secure disposal. Never put sensitive and confidential waste in any normal waste bins.

Systems and Software

47. All information processing systems which are to be used for storing and processing Council information must be formally authorised by IT. Information asset owners are responsible for ensuring new systems have the necessary validation checks and audit trails and also for ensuring user acceptance testing is carried out.

48. The Council's IT team will have overall responsibility for keeping the authority's anti-virus and other security software up to date.

49. User access to systems must be adequately controlled using complex passwords and appropriate access rights. User access rights must be regularly reviewed to ensure they are still appropriate.

50. Users must use a unique username and password for accessing the Council's network and information systems.

51. Users are responsible for keeping their passwords confidential at all times, and must not disclose passwords to anyone, including their line managers. Weak passwords must not be used.

52. Users must not attempt to access systems or records within systems which they have not been formally authorised to access.

53. Users must not bypass, disable or subvert system security controls.

54. Computer systems and software must only be used for purposes for which they are designated.

55. USB ports are restricted and must only permit the use of IT approved and encrypted devices. Active scanning will automatically check all media plugged into USB ports to ensure compliance with USB port restrictions

56. Only software authorised by IT shall be loaded onto the Council's computers.

57. Software must only be used in compliance with the terms of any contractual or licence agreements.

58. The Council will have sole ownership and copyright of all programs and data it has developed, unless there is a contrary prior written agreement otherwise.

59. Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is strictly forbidden.

60. All staff with IT access must undergo the Council's Information security e-learning refresher package. Managers will ensure this is part of a new employees' induction.

61. Managers must ensure that when any staff member leaves the Authority, all Council equipment (including their ID card) is returned. IT Service Desk must be informed of all leavers immediately to ensure network access is revoked.

62. All users must inform their manager if they detect, suspect or witness an incident which may be a breach of security.

63. All users must be aware that the network is monitored. IT Service Desk will monitor day to day access to ensure adequate protection against security threats, and where necessary, will collect evidence of misuse and unauthorised activity.

Information Handling

Building Security

64. All facilities that hold or process information must be suitably physically secured. This includes, but is not limited to -

    - The general office space will have controlled access, and logs recording access
    - Visitors to office facilities must be escorted at all times while in data processing areas
    - Visitor reception and pass procedures must be followed
    - IT servers and other sensitive equipment should be enclosed in secure locked areas if in general office areas

Storage

65. It is everyone's role to ensure that information is not put at risk of damage or theft, and is stored securely and access allowed only to those who need it for legitimate purposes and in accordance with the Data Protection Act 1998. For example all Council records are stored in secure buildings with access controls to the building and specific floors. The locations of any stored records are sited to avoid unauthorised access, damage, theft and interference. Electronic information should be stored on the Council network unless alternative storage (e.g. Cloud) is authorised by IT.

Other forms of Communication

66. Extra care must be taken when printing sensitive or confidential information or sending/receiving faxes. When sending sensitive or confidential information a test fax must be sent prior to sending the information or phone the organisation first to let them know what is being sent. In areas without multi-functional devices ensure printed sensitive or confidential information is not left unattended.

67. Voicemail may contain personal and sensitive or confidential information and therefore passwords must be kept secure.

Portable hardware including laptops, mobile devices & tablets

68. Portable hardware should be protected by a password or pin code.

69. Equipment taken off site must be locked away and kept out of sight when left unattended.

70. Users shall ensure that unauthorised persons are not able to view Council information on portable devices and shall protect access by locking computers when unattended. This policy also applies to staff accessing Council information on own devices.

71. Staff must ensure they do not leave portable media such as CDs that contains personal or sensitive information in drives.

Removable media

72. To prevent data loss, the use of USB devices such as portable hard drives and removable media (such as CDs, DVDs, memory sticks etc.) on Council PCs must not be used to store personal and sensitive or confidential information unless there is a business requirement to do so.

73. Staff must only use mobile media to transfer personal and sensitive or confidential Council information if there is a business requirement to do so and there is no other more secure means available e.g. Government secure GCSx email.

74. Only media purchased through the Councils IT service and with a sufficient level of encryption, may be used to temporarily hold personal and sensitive or confidential Council information.

Office/desk security

75. Staff must ensure that all personal and sensitive or confidential information is stored securely for example:

    - Personal and sensitive or confidential information including phone numbers, passwords, financial records, notes on meeting times, places and subjects are not left unattended
    - Mobile phones can contain sensitive or confidential personal information and have their call histories compromised and therefore must be password protected.

- Keys and access cards must not be left unattended as they can give intruders access to restricted areas
- Positioning of desks, furniture and visual display boards must be carefully considered to prevent sensitive or confidential information being visible to unauthorised people.
- Personal and sensitive or confidential information must not be left on white boards or notice boards.
- When leaving desks for short periods all users must use 'Ctrl, Alt and Delete' to lock computers. When leaving desks for long periods users must ensure they are logged off the network.
- All doors and windows must be closed outside office hours. Any open doors or windows during office hours must not allow unauthorised access to the building to take place.

Security and Breaches

76. Any loss or risk of loss of information, either actual or suspected, must be reported immediately to the relevant line manager. The Council will notify other parties, such as the Information Commissioner, as required or recommended by legislation and take action as appropriate. Under the Data Protection Act (DPA), although there is no legal obligation on data controllers to report breaches of security, we believe that serious breaches should be reported to the ICO. Further details can be found on the ICO website.

77. If staff suspect that a breach has occurred, this should be reported immediately to their line manager. Managers should liaise with the Head of Legal and Democratic Services to discuss the nature of the breach and how it should be taken forward.

Individuals' Rights

78. The Data Protection Act gives rights to individuals in respect of personal data held about them by others. These rights are:

    - Right of Subject Access;
    - Right to Prevent Processing Likely to Cause Damage or Distress;
    - Right to Prevent Direct Marketing;
    - Rights in Relation to Automated Decision Making;
    - Right to take action for compensation if an individual suffers damage by any contravention of the Act by the data controller;
    - Right to take action to rectify, block, erase or destroy inaccurate data.
    - Right to request that the Information Commissioner carries out an assessment of a data controller's processing of their data.

Data Subject Rights

79. Where appropriate, complaints about the way the Council processes an individual's personal information – especially those which highlight where a system or process could be improved - should be brought to the attention of the Data Protection Officer.

80. Individuals are entitled to request that the Council stop processing information they believe causes damage or distress. The Council has a legal obligation to review and respond to such complaints within 21 days, advising the individual if their compliant is upheld or rejected and the reasons for this.

81. Whilst data protection is everyone's responsibility, the Data Protection Officer will have overall responsibility for ensuring that the Council's procedures are up to date, and that the rights of data subjects are respected.

Right to Subject Access

82. Every individual has the right to request a copy of all the information held about them by the Council. This is known as a Subject Access Request.

83. A Subject Access Request must be answered within 40 calendar days. There may be situations where information about an individual is exempt from release. This could be because the individual's information is also the personal data of another person or it may be felt that the release of information may cause harm. The Freedom of Information/ Data Protection Officer will provide advice on exemptions to the release of information.

Disclosure of Personal Data

84. Requests for the disclosure of another person's personal data fall under either the Freedom of Information Act or the Environmental Information Regulations. All employees and Elected Members should exercise caution when asked to disclose personal data held on another individual to a third party.

85. Personal data can be legitimately disclosed in certain circumstances, such as:

    - Where the individual has given their consent
    - Where the disclosure is in the legitimate interests of the Council and the Act permits such disclosure without consent in relation to specific purposes.
    - Where the Council is legally obliged to disclose data
    - Where disclosure of data is required in relation to a contract which the individual has entered into.

86. Unless consent has been obtained from the data subject, information should not be disclosed over the telephone.

87. In addition, there are situations where personal data can, and indeed, must be proactively disclosed without a request having first been made, for example, to protect individuals. A judgement should be formed as to the reasonableness of disclosing the data according to the circumstances.

88. The Council reserves the right to disclose information under certain circumstances where allowed by law.

89. The Council will consider each request for disclosure individually. Where a disclosure takes place, the Council will only disclose the minimum amount required.

Roles and Responsibilities

Accountable Officer

90. The Chief Executive Officer for Ashford Borough Council is ultimately responsible for ensuring that all information is appropriately protected and that the Data Protection Act is adhered to.

General Responsibilities

91. The Council has a corporate responsibility for data protection, and is defined as the "Data Controller" by the Act.

92. Elected Members are each separately defined as "Data Controllers" in their capacity as ward members as well.

93. All employees and Elected Members are individually responsible for ensuring that their collection, storage, processing and destruction of data are in accordance with the Act. All employees and Elected Members have a duty to carry out regular accuracy checks of Personal Data in the normal course of Business.

Data Protection Officer

94. The Data Protection Officer is responsible for data protection issues and setting standards and procedures in relation to the Act, and acts as a liaison to other partner organisations.

Key Workers

95. A list of key workers from across the Council is available on the Intranet. This list should be consulted initially if any employees need support regarding data protection and the security of information.

Ensuring Compliance

96. In order to ensure it meets its obligations under the Data Protection Act, Ashford Borough Council will ensure that with relation to its employees and elected members:

- There is an individual with responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Persons wishing to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of how to make such an enquiry.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.

For Managers

97. All line managers must make sure that all persons that have authorised use of the Council's IT systems have adequate and appropriate understanding and training on:

- operating the technology and information systems provided
- understanding the security risks to their information systems
- using the security features provided within their information systems
- choosing, managing and protecting passwords and not passing them to others or leaving with their computer
- ensuring accounts are locked when absent from computers
- preventing the infection or spread of Malware and protecting data from the damage that Malware can cause
- identifying and protecting important, sensitive, personal or confidential data or records from loss, destruction and error
- applying agreed document classification and record retention schemes in accordance with the Council's Data Retention guidelines. These guidelines will be updated with input from services.
- only use Council supplied encrypted external storage devices
- ensuring the physical security of their desktop, laptop and other information assets
- identifying and reporting security incidents[3]

[3] An Information Security incident is an event that compromises the confidentiality, integrity or availability of information or information assets, having an adverse effect on security, reputation, performance or ability to meet regulatory or legal obligations

For All Staff

98. All employees should be aware of the Data Protection policy and the good practice contained within it relating to data protection and the management of electronic and non-electronic information.

For Contract Managers

99. These must ensure that any third parties or contractors operating on behalf of the Council are aware of the requirements around data protection, and to check, as appropriate, that they comply with them.

100. Information shall only be shared within the Council and with other organisations in line with the law and only where there is a need or obligation to do so, and consent has been given or legislation allows. Where there is a need to enable service delivery with external organisations the information sharing will be governed either under the terms of a contract or an information sharing or information access /disclosure agreement. The Council will also share information as required by law.

Support and Training

101. The Information Commissioner's Office (ICO) (https://ico.org.uk/) has prepared a detailed guide on the practicalities of dealing with the Data Protection Act 1998.

102. The ICO's role is to uphold information rights in the public interest. The ICO can take action to change the behaviour of organisations and individuals that collect, use and keep personal information.

103. The Data Protection Officer can also advise on all aspects of the Council's dealings with personal data and best practice, for example on the requirements around Subject Access Requests.

104. Ashford Borough Council will ensure that all staff are aware of the requirements of the Act, and that appropriate specific training is given to relevant staff within service areas on relevant aspects of Data Protection.

Accountability and Review

105. This policy, data protection arrangements and guidance will be reviewed every three years, unless there is a major change to the underlying regulations.

106. The ICO may use criminal prosecution, non-criminal enforcement and audit, depending on the circumstances. The ICO also has the power to serve a monetary penalty notice on a data controller.

107. Some of the options open to the ICO where there has been a more serious breach of the Data Protection Act include the ability to:

- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010;
- prosecute those who commit criminal offences under the Act.