Ashford Borough Council

DATA PROTECTION POLICY

Last updated: March 2019

Version History

Version	Date	Amendments	Reviewed/Approved
V1.00	March 2017	First Version	PCOURTINE
V2.00	March 2019	Revisions for GDPR/DPA18	TS/CH

Next review date: On or before March 2021

Author: Tom Swain

Contents

Introduction....4
Policy Statement....5
The Scope of this Document....6
Key Data Protection requirements....7
'Lawfulness, fairness and transparency'....7
'Purpose limitation'....8
'Data minimisation'....9
'Accuracy'....9
'Retention'....9
'Integrity and confidentiality'....10
Individuals' rights....11
Sharing personal data....12
Data processors....12
Records of processing activities....13
Data Protection Impact Assessments....14
Use of email, instant messaging and social media....14
Home and off-site working....15
Systems and software....16
Breaches and penalties....17
Relevant roles and responsibilities....18
Ensuring Compliance....18
Other documents....19
Questions....19
Review of this policy....19

Introduction

1. This policy provides Ashford Borough Council's (ABC) standards which must be maintained to comply with the UK's Data Protection Act 2018 (DPA18) and EU's General Data Protection Regulation 2016 (GDPR).

2. We are registered with the Information Commissioner's Office with registration number Z8344724.

3. ABC 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, we will not be able to fulfil these obligations whilst maintaining the confidence of service users.

4. This document is available to: all ABC Employees, Partners, Contractors, Agents and Elected Members.

5. Key Messages

    - ABC is a data controller and as such all Council Employees, Partners, Contractors, Agents and Elected Members have a responsibility for data protection.
    - Service Heads as the most senior/responsible individuals within each service are required to take on the role of Information Asset Owners (IAOs). Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why to data within their respective service. As a result they are able to understand and address risks to this information, and ensure it is only processed in line with data protection law.
    - Data protection applies to all the personal and "sensitive" special category data held by, and on behalf of, ABC. This information must be lawfully and fairly processed relying upon appropriate legal bases and the provision of suitable privacy notices.
    - You must only access personal data, client records, files and folders which you "need to know" in order to do your job. Unauthorised access is a criminal offence.
    - Safeguarding of people, at immediate risk of harm, over-rides data protection concerns.
    - All members of the public, employees and members, as data subjects, have statutory rights including the right of access to their data.
    - Data Protection training is a mandatory learning module all employees must complete as part of their inductions and revisit as a refresher module every two years.
    - You must report any suspected data breach of personal or sensitive data to the Data Protection Officer (DPO) immediately.
    - Make yourself aware of the additional statutory responsibilities on the Council, including the need for Privacy Notices, Data Processing Contracts, Records of Processing Activities and Data Protection Impact Assessments.

Policy Statement

6. Any personal information - however it is acquired, held, processed, released or destroyed - must be dealt with in a transparent manner that maintains the trust of the general public and our colleagues. We also need to ensure that we comply with our legal obligations when collecting and using personal data. In particular, we have to comply with the six "data protection principles", which are that personal data shall be:

    1) processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**)
    2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (**'purpose limitation'**)
    3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**)
    4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy**')
    5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, with due regard to the rights and freedoms of the data subject (**'storage limitation'** or **'retention'**)
    6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**).

    As a data controller we are responsible for, and need to be able to, demonstrate compliance with the above principles **('accountability')**.

7. Always be as careful with other people's personal information as you would expect others to be with yours. Good security is good practice and common sense.

8. ABC is also committed to preserving the confidentiality, integrity and availability of our information assets:

    - For sound decision making;
    - 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; and
- To safeguard against fraudulent activity.

9. This policy therefore also sets out our 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 unauthorised 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; and
    - Business requirements for the availability of information and information systems will be met.

The Scope of this Document

10. This policy applies to all ABC employees, partners, contractors, agents and elected members operating on our behalf or on our premises (referred to collectively as **employees** or **you**).

11. In addition elected members as representatives for the residents of their respective wards may act as data controllers in their own right, for example when dealing directly with requests received from constituents. ABC registers each elected member separately with the Information Commissioner's Office.

12. This policy applies to all personal data and other confidential or sensitive information held by ABC, in whatever form. This includes information stored as follows:
    - Hardcopy documents on paper and sent by fax
    - Electronic information stored on computers, remote servers, mobile devices, tapes, microfilm, CDs, external disks, USB storage devices and any other electronic storage medium; and
    - Verbal information (face to face conversations and over the telephone).

13. The policy sets out ABC's legal responsibilities and how you must act when processing personal and other confidential data to ensure ABC complies with those responsibilities. Everyone at ABC is responsible for making sure that ABC complies with its obligations and this means there are certain steps you must make sure you always take when dealing with personal data.

14. “Personal data” means any information about an identifiable living individual. This includes, for example, an individual’s contact details, such as name, address, email address and telephone numbers. It can include information about individual’s council tax payments, web browsing history and their opinions and beliefs. Images and call recordings can also be classed as personal data so consideration must be given to this information when reading this policy. In relation to colleagues, personal data includes job role, salary and benefits information and performance reviews.

15. Some information is designated as “special category personal data”. This is information that relates to an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. Due to the private nature of special category personal data, stricter rules apply.

16. As well as personal data, this policy also applies to confidential information handled by ABC. This may include any commercially sensitive information, such as information relating to commercial proposals or current negotiations; information relating to security, investigations and proceedings, and any information provided in confidence.

Key Data Protection requirements

‘Lawfulness, fairness and transparency’

17. We must be clear and open about what we intend to do with individuals’ personal data. Privacy notices are a crucial tool to aid in our data protection compliance, spelling out to the data subject at the point where their personal data is collected, in a concise, transparent and easily accessible form, what they can expect to happen to their data. The following information should be provided to the data subject:
    a. The identity and contact details of the data controller and the data protection officer;
    b. The legal basis relied upon to legally process;
    c. A clear description of the reason the information is collected;
    d. Whether we are going to share it with anyone else;
    e. The period or criteria used to determine such period for which the data will be held;
    f. Any intention to transfer personal data outside the European Economic Area;
    g. Information on the individual’s rights. For example, if relying upon consent as the legal basis to process, how this consent can be withdrawn;
    h. The existence of any automated decision making; and
    i. The right to lodge a complaint with the supervisory authority (ICO)

18. This information is provided in different ways depending on how people give us their information, for example:
    a. website privacy policies for information collected through online forms;

b. conversations with people who telephone us; and
c. hardcopy privacy notices for individuals who do not want to use online forms.

19. We must always have a legal basis for collecting and using personal data; generally the legal basis for processing by us as a public authority will be one of the following:
    a. **Public task:** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the council;
    b. **Legal obligation:** processing is necessary for compliance with the council's legal obligation;
    c. **Contract:** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps on their request prior to entering into a contract.

    We may also on occasion process personal data relying upon the following circumstances:
    d. **Consent:** where the data subject has given consent to the processing of their personal data for one or more specific purposes;
    e. **Legitimate interests:** where processing is necessary for the purposes of the legitimate interests pursued by us or by a third party. This legal basis is not open to us when performing our statutory tasks; however, where we are operating on a commercial basis, this legal basis may be utilised; and
    f. **Vital interests:** where processing is necessary in order to protect the vital interests of the data subject or of another individual. For example, protecting someone or their property from imminent harm or damage.

20. When special category data is collected, we will also need to ensure a secondary condition is met from within Article 9 (2) of the GDPR (processing of special categories of personal data). If in doubt please consult with the Data Protection Officer.

21. You should note that it is a criminal offence to knowingly or recklessly obtain or disclose personal data without ABC's consent, for example by using the data used at work for personal use. Employees should not process any personal data unless they are sure that they are authorised to do so; failure to do so may result in liability for non-compliance with data protection legislation for ABC and the employees involved.

'Purpose limitation'

22. Personal data should only be used for the purpose for which it was collected. If personal data is to be used for a new purpose not compatible with the previous purpose the data subject should be consulted, provided with an updated privacy notice and, if necessary, any required consent re-gained.

23. The principle of purpose limitation is fundamentally linked with that of the principle of processing personal data fairly, lawfully and transparently and as such the data subject must be provided with a description of the specific purpose for which any collected personal data

is to be used. This allows for personal data to be collected in a clear and open manner aiding with our accountability requirements and preventing function creep.

'Data minimisation'

24. We should only ever collect and process the minimal amount of personal data needed to fulfil the operational needs associated to the purpose of collection or to comply with any legal requirements.

25. Personal data shall only be collected if it is adequate, relevant and strictly limited to what is necessary to fulfil the desired purpose.

'Accuracy'

26. We must make sure that the personal data we hold is accurate, relevant and up-to-date. This means that:
    a. We should check personal data is correct when we first receive it. For example, if you take someone's telephone number, make sure that it has the correct number of digits and read it back to them to check it is correct.
    b. We should periodically review personal data we hold to make sure it stays up-to-date. For example, if you hold an address on file that has been the same for a number of years, you should check whether the person has now changed addresses.
    c. If we receive a request to correct inaccurate personal data, we should correct it straight away. For example, if someone phones you to tell you the email address you hold for them is incorrect, you should change this immediately on our systems.

'Retention'

27. We must ensure that we delete or destroy personal data securely when we no longer need it, in accordance with our Data Retention Policy and in line with the details provided in any privacy notices. Electronic documents and devices should be destroyed by the IT team, and paper documents should be placed in confidential waste bins.

'Integrity and confidentiality'

28. All managers and staff are responsible for ensuring that personal data is held securely at all times. If we don't keep personal data secure, it can lead to real harm and distress for individuals.

29. When deciding what level of security is appropriate, we need to look at the potential risks arising out of accidental disclosure of the relevant data. This includes thinking about the value, sensitivity and confidentiality of the data involved and the likely harm that could result if we don't handle it properly. For example, information about people's health will require a higher level of security than a list of email addresses.

30. Note that the requirements to keep information secure apply to information both within and outside ABC's premises.

31. As a minimum, you should always take the following steps to make sure that data is kept securely:

    a. Make sure that all systems are password-protected and that only authorised personnel can access the systems. Keep your passwords secure at all times, including your password to your voicemail.
    b. Make sure that passwords you use to access our systems or devices are "strong" passwords, in line with our password guidance.
    c. Ensure that only employees who need access to particular personal data to do their jobs can access it. If you think you have access to data that you don't need to see, contact the DPO immediately.
    d. Don't leave devices unattended and make sure that electronic files are inaccessible when left unattended. For example, lock your screen if you leave your desk and don't leave hardcopy files in open view.
    e. When you use portable devices to store personal data, you must be very careful and make sure devices are always encrypted. Use of portable devices should follow the Bring Your Own Device policy.
    f. Make sure you safely dispose of records when they are no longer required, in accordance with the sections above headed "Accuracy'', ''Retention" and our Data Retention Policy.
    g. Take care when printing or photocopying sensitive or confidential information and sending or receiving faxes. Make sure you do not leave printing unattended and always send test faxes first to ensure you are using the correct number.
    h. If you take equipment, such as laptops, off-site, these should always be locked away and kept out of sight when left unattended. Make sure that people off the premises cannot see confidential information you are dealing with, for example by looking at a laptop screen over your shoulder.
    i. Don't leave portable media such as CDs that contain personal or confidential information in CD drives.

j. Make sure that you do not discuss any ABC business in public, either face-to-face or on the phone.
k. Take good care of your keys and access fobs and do not leave these unattended. If you lose keys or access fobs, please inform the DPO and the Facilities Management team immediately.
l. Always wipe white boards and remove personal data from notice boards when you have finished using them.
m. Make sure all doors and windows at ABC's premises are closed outside of business hours. If windows and doors are open during business hours, they should not allow unauthorised access to the building.
n. If you are in charge of visitors to the building, make sure they are escorted at all times and their access is logged, including times in and out, as per the visitors procedure.
o. Always lock away hardcopy files in locked cupboards when you are not using them.

Individuals' rights

32. Individuals have a number of rights under data protection law. ABC must comply with those rights.

33. In particular, individuals have a legal right to receive a copy of their personal data (known as "subject access rights"). If someone requests a copy of their personal data, we must respond within one calendar month.

34. Please note that opinions about someone constitute their personal data so everyone has a right to see recorded opinions about themselves. Bear this in mind if you are ever recording opinions about another individual. Opinions recorded on a file must be carefully and professionally expressed to avoid causing embarrassment to ABC if a subject access request is made for that data.

35. The complete list of individual's rights are as follows:

    a. the right to be informed;
    b. the right of access;
    c. the right to rectification;
    d. the right to erase;
    e. the right to restrict processing;
    f. the right to data portability;
    g. the right to object; and
    h. rights in relation to automated decision making and profiling.

    The councils individual rights policy provide a detailed explanation of what each of these rights involves so that all employees are able to recognise these rights if an individual seeks to exercise them. The policy also explains the timeframes for responding to requests and the consequences if we fail to respond as we should.

Sharing personal data

36. We recognise the need to share personal and sensitive data with other partner organisations in order to safeguard the vulnerable and provide effective and efficient services.

37. If you need to share personal data with a third party for any reason, you must always comply with our Data Sharing Protocol and follow our Data Sharing Checklist.

38. We are signatories to the Kent & Medway Information Sharing Agreement which provides a framework to enable a number of organisations and public bodies across Kent and Medway to share personal information in line with agreed data sharing protocols.

39. When we collect personal data from individuals, we must be clear and open about whether we are going to share that data with third parties. If we are going to share personal data with third parties, we must explain why we need to do this.

40. We are sometimes asked to share personal data with the police, regulators, banks and other local or central government bodies for the purposes of crime prevention and detection, fraud investigations and to verify information relating to credit and job applications. Although exemptions to the DPA18 and GDPR may apply we must avoid taking a blanket approach and assess each request on its individual merit.

41. We cannot send personal information, or allow people to access personal information, outside the European Economic Area, unless certain contractual requirements or information security conditions are met. If you are working on a project that might involve sending personal information outside the UK and if you are unsure about whether you have met these conditions, you must refer to the DPO.

42. Please also note that requests for information may fall within the Freedom of Information Act and/or the Environmental Information Regulations. Please see the Freedom of Information page for details on how to deal with these requests.

Data processors

43. When we pass personal data to third party suppliers who use the data to provide services to us, they will be a “data processor” on our behalf. We must ensure that they have adequate measures in place to keep personal data secure and we must ensure that a written contract is in place with the supplier.

44. Any data processor will need to agree to process data only in accordance with data protection laws and, in particular, on the following conditions, which must be included in a written contract:

a. the Processor shall only process the Data (i) on the written instructions from Ashford Borough Council (ii) only process the Data for completing the Services and (iii) only process the Data in the EU with no transfer of the Data outside of the EU (Article 28, para 3(a) GDPR);
b. ensure that all employees and other representatives accessing the Data are (i) aware of the terms of the Agreement and (ii) have received comprehensive training on Data Protection Laws and related good practice, and (iii) are bound by a commitment of confidentiality (Article 28, para 3(b) GDPR);
c. Ashford Borough Council and the Processor have agreed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, complying with Article 32 of GDPR, (Article 28, para 3(c) GDPR);
d. the Processor shall not involve any third party in the processing of the Data without the consent of Ashford Borough Council. Such consent may be withheld without reason. If consent is given a further processing agreement will be required (Article 28, para 3(d) GDPR);
e. taking into account the nature of the processing, assist Ashford Borough Council by taking appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of Ashford Borough Council's obligation to respond to requests from individuals exercising their rights laid down in Chapter III of GDPR – rights to erasure, rectification, access, restriction, portability, object and right not to be subject to automated decision making, etc. (Article 28, para 3(e) GDPR);
f. assist Ashford Borough Council in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and when necessary consultation with the ICO, etc. taking into account the nature of processing and the information available to the Processor (Article 28, para 3(f) GDPR);
g. at Ashford Borough Council's choice safely delete or return the Data at any time. [It has been agreed that the Processor will in any event securely delete the Data at the end of the Services.] Where the Processor is to delete the Data, deletion shall include destruction of all existing copies, unless there is a legal requirement to retain the Data. Where there is a legal requirement, the Processor will, prior to entering into this Agreement, confirm such an obligation in writing to Ashford Borough Council. Upon request by Ashford Borough Council the Processor shall provide certification of destruction of all Data (Article 28, para 3(g) GDPR); and
h. make immediately available to Ashford Borough Council all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for, and contribute to, any audits, inspections or other verification exercises required by Ashford Borough Council from time to time (Article 28, para 3(h) GDPR).

Records of processing activities

45. ABC, as a data controller, shall maintain a record of processing activities under its responsibility. This record must contain:

a. Our name and corporate contact details, together with the contact details of our Data Protection Officer;
b. The purposes of processing the personal data;
c. A description of the categories of data subjects and of the categories of personal data;
d. The categories of recipients to whom the personal data have been or will be disclosed including, where applicable, recipients in third countries or international organisations;
e. Details of suitable safeguards if the data is transferred outside the EU;
f. Via our Records Retention Schedules the envisaged time limits for erasure of the different categories of data; and
g. A general description of the technical and organisational security measures in place to protect this data – it should be noted that access for security reasons to such data will be extremely limited.

46. These details may be requested by the ICO at any time and as such will require regular updating to maintain an accurate representation of our processing activities.

47. These records will be the responsibility of the respective Head of Service as IAO for each service to ensure they are maintained. These records will be scrutinised by the data protection team and Information Governance group periodically and/or when required.

Data Protection Impact Assessments

48. Data Protection Impact Assessments (DPIAs) are tools which can help identify the most effective way to comply with its data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow ABC to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. DPIAs are an integral part of taking a 'privacy by design' approach, and are a legal requirement whenever a 'process is likely to result in a high risk to the rights and freedoms of natural persons'. A DPIA template is available on the intranet.

Use of email, instant messaging and social media

49. Email is an essential tool for conducting day to day business. However, sending information by email presents certain security risks. For example, emails can be intercepted or accidentally sent to the wrong recipient. Incoming emails may contain links that are used to hack our systems through phishing attacks or similar.

50. Sending an email to the wrong person or to an out of date email address can have serious consequences, so it is important to always check before you send that the email is addressed to the correct individuals and that the addresses are current. The 'external recipients mailtip'

is turned on by default and will show a warning at the top of any message should an external email address be inserted. However If you regularly email sensitive or confidential data (especially to people outside the Council), you should also consider whether or not to turn off the auto-complete function in Outlook (see the intranet on how to do this).

51. An email address can be classified as personal information and as such the same care should be taken with it as with any other personal information. This includes not sharing it with unauthorised individuals, so it is essential to **use** the **Blind Carbon Copy** (**BCC**) feature **when sending** email messages to multiple external recipients especially where those recipients do not know one another. When you place email addresses in the **BCC** field of a message, those addresses are invisible to the recipients of the email and thus any personal information contained within the email address is protected.

52. All emails that are used to conduct or support official ABC business should be sent using an "@ashford.gov.uk" address. You must not use non-work email accounts to conduct, support or discuss official ABC business.

53. You must not open attachments or click on hyperlinks within e-mails from unknown sources. If an email looks suspicious, please inform the DPO and forward the email to the IT team.

54. ABC's official disclaimer along with a link to its privacy notice is automatically added to all emails sent to external addresses – this is an important security feature and should not be altered.

55. When forwarding or replying to a message, consider the chain of messages that precede it and whether these need to be sent on. Generally, you should make sure that you do not send personal or confidential data by email unless you need to or have been authorised to do so.

56. Emails that contain personal or confidential data, particularly sensitive data, should be password-protected or encrypted. If you are sending attachments containing confidential data, the attachments should be password-protected and the password sent in a separate email.

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

Home and off-site working

58. When working from home or remotely from other locations, you must take the steps set out in this section as a minimum to protect personal and confidential data whilst off-site.

a. All remote working must be carried out in compliance with ABC's remote working and portable device guidance, health and safety policy and conditions of service and must be authorised by your line manager.
b. Any laptop or other device that is taken off ABC premises must be encrypted and allocated to the user.
c. All necessary precautions must be taken to ensure the security of hardcopy documents that are taken off ABC premises. For example, you must make sure that you do not leave hardcopy documents in open view when off-site.
d. You must make sure you only use personal data you take off-site for official ABC business. Do not take any personal data off-site without authorisation from your line manager.
e. If you need to dispose of personal data when off-site, you must shred hardcopy information and must contact the IT team to dispose of any IT equipment or electronic files. If you cannot securely dispose of files, information or equipment at your remote working place, you must take the information securely to ABC's premises to destroy them.

Systems and software

59. It is important that all of our IT systems and software are as secure as possible and are used appropriately to ensure personal data stored in those systems and software is protected.

60. All information processing systems which are to be used for storing and processing ABC information must be formally authorised by IT. You must not install any software on any ABC computers or devices which has not been authorised. 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. Depending on the scope of any new software it may be necessary to carry out a Data Protection Impact assessment.

61. ABC's IT team will have overall responsibility for keeping the authority's anti-virus and other security software up to date. If any software on your computer or any other device is out-of-date, please make sure that you contact IT so this can be updated.

62. User access to systems must be adequately controlled using appropriate access rights and protected by passwords in line with our password guidance. User access rights must be regularly reviewed to ensure they are still appropriate. If you think yours or someone else's access rights need updating please notify the DPO and the IT team.

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

64. Users must not, and must not attempt to, bypass, disable or subvert system security controls.

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

66. Only IT approved and encrypted USB memory devices should be used ensuring that any personal data that may be present is encrypted during transport. Before any new memory device is plugged into any ABC system it is essential it is scanned for threats by the IT team.

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

68. ABC will have sole ownership and copyright of all programs and data it has developed, unless there is a contrary prior written agreement.

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

70. All employees with IT access must undergo ABC's data protection e-learning module and complete the refresher package at least every two years. Managers will ensure this is part of a new employee's induction.

71. Managers must ensure that when any employee leaves ABC, all ABC equipment (including their ID card) is returned. IT Service Desk must be informed of all leavers immediately to ensure network access is revoked.

72. 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.

Breaches and penalties

73. Despite everyone's best efforts, issues may sometimes arise. For example, we may lose personal data accidentally; someone may steal personal data or attack our systems; or our IT equipment may fail and result in data being lost or accessed by a third party.

74. If there is a security breach, we need to act quickly and appropriately to manage the breach and limit the effects and damage it causes. Where a breach poses a risk to the rights or freedoms of individuals we are obligated to report this to the ICO. Furthermore this reporting must happen within 72hrs of discovery.

75. Even if the decision is taken by the DPO not to report, all breaches should be logged internally, investigated, and any required remedial actions taken. Learning from previous breaches aids with the prevention of future breaches and as such learning points must be circulated.

76. Any security breach, either actual or suspected, must be escalated immediately as set out in the Data Security Breach Management Policy.

77. The consequences of a security breach can be severe. They can include:

    a. Real harm and distress for the individuals involved.
    b. Reputational consequences for ABC and a loss of public trust in ABC.
    c. Legal enforcement action being taken by the ICO.
    d. Compensation claims being made by individuals.

78. It is therefore essential that in the event of a breach you follow the steps on the Data Security Breaches page and keep an accurate record of the circumstances.

Relevant roles and responsibilities

79. Everyone at ABC is responsible for ensuring they comply with this policy and with all other data protection and security policies. There are some specific roles it may be useful for you to be aware of, as follows:
    a. The Chief Executive for ABC is ultimately responsible for ensuring that all information is appropriately protected and that data protection law is adhered to.
    b. The DPO is responsible for data protection issues and setting standards and procedures in relation to data protection laws. The DPO also acts as a liaison with other partner organisations and with the ICO if necessary. The DPO is required to act and advise independently.
    c. Service Heads, as the most senior/responsible individuals within each service, are required to take on the role of Information Asset Owners (IAOs). Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why to data within their respective service. As a result they are able to understand and address risks to this information, and ensure it is only processed in line with data protection law.
    d. ABC designates certain employees as "key workers". Key workers have received additional training and can be consulted if you need support or have questions regarding data protection and information security.

Ensuring Compliance

80. Key workers and other senior employees may be responsible for ensuring data protection compliance across their Services. Those employees should act in accordance with the Compliance Monitoring Protocol and should escalate any queries to the DPO.

81. All employees must undergo data protection training as part of their inductions and once every two years thereafter. If you have not received data protection training, please inform your line manager.

82. If you are responsible for managing the relationship and/or contract with a third party or contractor operating on ABC's behalf, you must make sure that those third parties or contractors are aware of this policy and of their obligations around data protection. You must also periodically check that they are complying with those obligations, for example through periodic audits.

83. ABC has an internal officer lead Information Governance Group who with the aid of the Data Protection Officer will monitor compliance with the policy.

Other documents

84. Please also take note of ABC's other data protection documents which will help you comply with the policy. These include:
    e. Data Protection Top Tips
    f. Data Sharing Protocol
    g. Data Sharing Checklist
    h. Kent and Medway Information sharing agreement
    i. Data Retention Policy
    j. Individual rights
    k. Data Security Breaches
    l. Freedom of Information Guidance
    m. Freedom of Information Top Tips

Questions

85. If you have any questions about this policy, any of the other policies listed above or your data protection obligations, please contact the DPO.

Review of this policy

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