Agenda Item No:

Report To: Cabinet

Date of Meeting: 24 November 2022

Report Title: Data Protection Policy Suite (Periodic Review)

Report Author: Tom Swain
Job Title: Governance and Data Protection Officer

Portfolio Holder: Cllr. Peter Feacey
Portfolio Holder for: Portfolio Holder for Policy and Performance

Summary:

We need to collect and use certain personal 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 our service users and fulfilling our data protection obligations.

A robust Data Protection Policy Suite is therefore required to ensure our data protection obligations are documented, met and promoted to all.

The councils current Data Protection Policy Suite was reviewed and agreed by Members in March 2019.

To ensure our Data Protection Policy Suite remains relevant and fit for purpose it requires a periodic review. This report acts as a reviewing opportunity, with amends made to reflect any changes to the legislative data protection landscape and any best practice guidance issued by the supervisory authority (ICO) since the policy was last reviewed.

Key Decision: NO

Significantly Affected Wards: None

Recommendations: **The Cabinet is recommended to:-**

I. **Review and approve the amended Data Protection Policy Suite**
II. **Authorise the Data Protection Officer, in consultation with the Portfolio Holder, to approve minor amendments to the policy in-line with working arrangements and or legislative change.**

Policy Overview:	Revised Data Protection Policy Suite, with amends made to reflect any changes to the legislative data protection landscape and any best practice guidance issued by the supervisory authority (ICO) since the policy was last reviewed.
Financial Implications:	None
Legal Implications:	Required to ensure the council complies with its obligations as a Data Controller in line with the Data Protection act 2018 and UK GDPR.
Equalities Impact Assessment:	Not Required
Data Protection Impact Assessment:	Not Required
Exempt from Publication:	NO
Background Papers:	None
Contact:	Tom Swain – Governance and Data Protection Officer tom.swain@ashford.gov.uk – Tel: (01233 330432)

Agenda Item No.

Report Title:

Introduction and Background

1. The Council collects and uses a huge amount of personal data and has statutory obligations in respect of that personal data. We have a number of data protection related policies and procedures in place making up our policy suite , including:

    - Data Protection Policy;
    - Breach Management Policy;
    - Individual Rights Policy;
    - Data Sharing Protocol;
    - Data Protection Impact Assessment template;
    - Data Protection Compliance Monitoring Protocol

2. To ensure our Data Protection Policy Suite remains relevant and fit for purpose it requires a periodic review. This report acts as a reviewing opportunity, with amends made to reflect any changes to the legislative data protection landscape and any best practice guidance issued by the supervisory authority (ICO) since the policy was last reviewed.

Proposal

3. The Data Protection Policy Suite has been reviewed and amended taking into account:

4. The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, which amended the DPA 2018 and merged it with the requirements of the EU GDPR to form a new, UK-specific data protection regime that works in a UK context. This new regime is known as the ‘UK GDPR’, replacing GDPR.

5. The Data Protection (Charges and Information) (Amendment) Regulations 2019, which exempted the processing of personal data by members of the House of Lords, elected representatives and prospective representatives – this includes local authority councillors – from the requirement to register as separate data controllers with the ICO. All other data protection obligations remain.

6. The addition of a Senior Information Risk Owner (SIRO) to the relevant roles and responsibilities section of the Data Protection Policy. The SIRO will be a designated member of the Directorate with overall responsibility for the organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation. The SIRO for ABC is the Monitoring Officer.

7. Amendment to the council's Data Protection Impact Assessment (DPIA) template to reflect that recommended by the ICO.

8. General amends to the policy to bring it up-to-date.

Consultation Planned or Undertaken

9. The revised policy has been drafted by the data protection team, reflecting any changes to the legislative data protection landscape and any best practice guidance issued by the supervisory authority (ICO) since the policy was last reviewed.

Reasons for Supporting Option Recommended

10. A robust Data Protection Policy Suite is required to ensure our data protection obligation are documented, met and promoted to all.

11. A failure to have a current regularly reviewed Data Protection Policy Suite would potentially place the council in a vulnerable position which could result in financial and reputational damage.

Next Steps in Process

12. Once approved by Cabinet this revised Data Protection Policy Suite will replace its predecessor as the Council's suite of information security policies.

Conclusion

13. We need to collect and use certain personal 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 our service users and fulfilling our data protection obligations.

14. The lawful and appropriate treatment of personal data is vital to our successful operations and essential to maintaining confidence between the council and our service users. The council therefore fully endorses and is committed to its data protection obligations as spelt out within the Data Protection act 2018 and UK GDPR.

15. A regularly reviewed policy suite is a key pillar to this, necessary to facilitate this objective.

Portfolio Holder's Views

16. A robust, regularly reviewed Data Protection Policy Suite is essential to ensure our data protection obligations are documented, met and promoted to all.

17. We are committed to our data protection obligations as spelt out within the Data Protection act 2018 and UK GDPR, ensuring the personal data of our service users is appropriately protected, legally processed and the rights and freedoms of the individuals are maintained.

Contact and Email

18. Tom Swain – Governance and Data Protection Officer
tom.swain@ashford.gov.uk – Tel: (01233 330432)

Ashford Borough Council

DATA PROTECTION POLICY

Last updated: December 2022

Version History

Version	Date	Amendments	Reviewed/Approved
V1.00	March 2017	First Version	PCOURTINE
V2.00	March 2019	Revisions for GDPR/DPA18	TS/CH
V3.00	December 2022	General revisions for UK GDPR	TS/CH

Next review date: On or before January 2025

Author: Tom Swain

Contents

Definitions

Some of the terms used in this policy have very specific meanings. These include:

I. **'data protection law**' means all applicable data protection and privacy legislation in force from time to time in the UK including the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR); the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended and the guidance and codes of practice issued by the Information Commissioner or other relevant regulatory authority;

II. **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

III. **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

IV. **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

V. **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

VI. **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

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 the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR).

2. We are registered as a Data Controller 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 our 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 area and are required to take on the role of Information Asset Owners (IAOs) for their respective service area. 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 (vital interest).
    - 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 e-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 Team immediately.
- You should make yourself aware of the additional statutory responsibilities on the Council, including the need for Privacy Notices, Data Processing clauses in 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. (**'purpose limitation'**);
    3) adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed (**'data minimisation'**);
    4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is being processed, is erased or rectified without delay (**'accuracy**');
    5) kept in a form which permits identification of a data subjects for no longer than is necessary for the purposes for which the personal data is being processed. (**'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.
    - 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. From 1 April 2019, the

Data Protection (Charges and Information) (Amendment) Regulations 2019 exempted the processing of personal data by elected representatives and prospective representatives from the requirement to register as a Data Controller with the supervisory authority. **All other data protection obligations remain**.

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
    - 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, heightened data protection obligations 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 UK or countries with UK adequacy regulations (countries in the EEA and countries, territories or sectors covered by existing EU 'adequacy decisions);
    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 regional 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 of the UK GDPR (processing of special categories of personal data). If in doubt please consult with the Data Protection Team.

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 individual 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, and you are sure the request has been made by the related data subject, we should correct it straight away. For example, if someone phones you to tell you the email address you hold for them is incorrect, subject to appropriate identity checks, 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 (available on the SmartHub) 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 the 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, the councils systems have appropriate password criteria in place to ensure this happens.
    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 speak to your line manager or the Data Protection Team.
    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. Make sure you do not leave printing unattended or leave sensitive documents in the copier.
    h. If you take equipment, such as laptops, off-site, or away from your remote working location 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. Make sure that you do not discuss any ABC business in public, either face-to-face or on the phone.
j. 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 Data Protection team and the Facilities Management team immediately.
k. Always wipe white boards and remove personal data from notice boards when you have finished using them.
l. 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.
m. 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.
n. 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, subject to exemption. 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.

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, the collection of a tax and to verify information relating to credit and job applications. Although exemptions to the DPA18 and UK 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 UK or countries with UK adequacy regulations (countries in the EEA and countries, territories or sectors covered by existing EU ‘adequacy decisions), 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 Data Protection team.

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 on the SmrtHub 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 (Article 28 UK GDPR):

    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 UK or countries with UK adequacy regulations (countries in the EEA and countries, territories or sectors covered by existing EU 'adequacy decisions);
    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;
    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 UK 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;
    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 – rights to erasure, rectification, access, restriction, portability, object and right not to be subject to automated decision making, etc;
    f. assist Ashford Borough Council in ensuring compliance with the obligations pursuant to Articles 32 to 36 of UK 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;

g. at Ashford Borough Council's choice safely delete or return the Data at any time. 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; and
h. make immediately available to Ashford Borough Council all information necessary to demonstrate compliance with the obligations laid down under any processing agreement and allow for, and contribute to, any audits, inspections or other verification exercises required by Ashford Borough Council from time to time.

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 UK or countries with UK adequacy regulations (countries in the EEA and countries, territories or sectors covered by existing EU 'adequacy decisions);
    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 our 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'. See our DPIA template or contact the Data Protection team for more information.

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.

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 Data Protection team 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 the IT department. 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 the system specific password criteria. 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 Data Protection team 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 Data Protection team 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 found within the Data Security Breach Management Policy.

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 Data Protection Officer (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. The DPO for ABC is the Head Of Policy and Performance.
    c. The Senior Information Risk Owner (SIRO) a designated member of the Directorate with overall responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation. The SIRO for ABC is the Monitoring Officer.
    d. 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.
    e. The Data Protection team, who can be consulted if you need support or have questions regarding data protection and information security.

Ensuring Compliance

80. The Data Protection team and 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 Data Protection team.

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 team will monitor compliance with this 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:
    a. Individual Rights Policy
    b. Data Security Breach Management Policy
    c. Data Protection Impact Assessment Template
    d. Data Sharing Protocol
    e. Data Protection Compliance Monitoring

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 Data Protection team.

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.

Ashford Borough Council

Individuals Rights Policy

1 Introduction

1.1 Under data protection legislation individuals have a number of rights in relation to their personal data. This policy provides an overview of individuals' rights and explains the procedures which Ashford Borough Council (referred to in this policy as, **Ashford**, **we**, **us**, or **our**) requires all employees and contractors (referred to in this policy collectively as **employees or you**) and councillors to comply with if an individual makes a request to exercise their data protection rights.

1.2 If you have any questions about this policy, please raise them with the data protection Team, at the following contact details:

Email: FOI@ashford.gov.uk

Address: Civic Centre, Tannery Lane, Ashford, Kent, TN23 1PL

2 What rights do individuals have under data protection law?

2.1 Under the UK General Data Protection Regulation (**UK GDPR**) individuals have the following rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erase;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights in relation to automated decision making and profiling.

2.2 The sections below 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.

3 The right to be informed

3.1 Individuals have a right to be informed about how we will use and share their personal data. This explanation must be provided to individuals in a concise, transparent, intelligible and easily accessible format. Privacy notices must be written in clear and plain language and must be provided free of charge.

3.2 We must ensure that we provide privacy notices to individuals at the point where we collect personal data from them if we are collecting personal data directly. If we obtain personal data from a third party then the information must be provided to individuals within one month or, if earlier, at the point of first contact with the individual or before personal data is disclosed to a third party.

3.3 The UK GDPR sets out a list of specified information that must be provided to individuals in privacy notices. We must therefore ensure that all privacy notices contain this mandatory information.

3.4 We satisfy this requirement by ensuring that appropriate privacy notices are included at all data collection points.

3.5 We have the following privacy notices that address our personal data use:

- employee privacy notice;
- recruitment privacy notice;
- public facing privacy notice which is published on our website and addresses the use of personal data by us in the majority of our service lines;
- task specific privacy notices.

4 Right of access – Known as a Subject Access Request

4.1 Under the right of access, individuals have a right to:

- obtain confirmation of whether we are processing their personal data;
- access their personal data; and
- information regarding how their personal data is being used by us.

4.2 The purpose of the right of access is to allow individuals to access their personal data so they are aware of and can verify the lawfulness of the processing carried out by us.

4.3 When an access request is received we must provide a copy of all personal data to the individual unless an exemption applies. There are a number of exemptions that may apply. This includes personal data that is subject to legal privilege and personal data that relates to third parties, which must be redacted so as not to breach the third parties data protection rights. This also applies where CCTV footage and call recordings include third parties, which may not be shared unless we have the necessary consents from the third parties.

4.4 A reasonable and proportionate search must be carried out to locate all relevant personal data and then a review of all documentation will need to be completed before sending relevant information to the individual.

4.5 We must respond to a request to exercise the right to access **within one month** of receiving the request in writing. Whilst we can ask a data subject to complete

a form or clarify any specific information in order to assist us in responding to the request, we cannot make our response conditional on receiving the request in a prescribed form, nor can we delay a response until this is received.

4.6 If a request for access is received you must contact the Data Protection Team immediately.

5 Right to rectification

5.1 Individuals have a right to have any inaccurate or incomplete personal data rectified.

5.2 If we have disclosed the relevant personal data to any third parties we are also responsible for taking reasonable steps to inform those third parties of the rectification where possible.

5.3 We have an obligation to ensure that the personal data we hold is accurate, so we should still verify that the request for rectification is valid and accurate, for example we should request to see reasonable evidence of any change, if appropriate.

5.4 If we dispute that the personal data is inaccurate then it will be necessary to go back to the individual and explain why the personal data is not being rectified. Individuals should also be informed at this point that they have a right to complain to the Information Commissioner's Office if they do not agree with this decision.

5.5 If you receive a rectification request and you are concerned it goes beyond a business as usual request or are unable to confirm the identity of the individual making the request you must contact the Data Protection Team immediately.

6 Right to erasure

6.1 Individuals have a right to request that certain personal data held by us is erased. This is also known as the "right to be forgotten". **This is not a blanket right** to require all personal data to be deleted. Rather the right will be triggered in the following circumstances:

- if we are continuing to process personal data beyond the period when it is necessary to do so for the purpose for which it was originally collected
- if we are relying on consent as the legal basis for processing and the individual withdraws their consent (usually this is not the case for our processing but is relevant for some activities);
- if we are relying on legitimate interest as the legal basis for processing and the individual objects to this processing and there is no overriding compelling ground which enables us to continue with the processing. *Please note that as a local authority, the circumstances in which we would be relying on the legitimate interest grounds for processing are restricted as legitimate interests may not*

be relied upon when we are acting in the performance of our public function and tasks;

- if the personal data has been processed unlawfully (i.e. in breach of the requirements of the UK GDPR or DPA 18); or
- if it is necessary to delete the personal data to comply with a legal obligation.

6.2 There are some exemptions to the right to erasure so even if one of the triggers above is met it may not be necessary to erase the relevant personal data. If information is required to exercise or defend legal claims then it is not necessary to delete the personal data. We are also permitted to retain personal data where there is a public interest task which requires the personal data to continue to be processed.

6.3 If you receive a request to erase personal data you must contact the Data Protection Team immediately.

7 Right to restrict processing

7.1 Individuals have a right to block the processing of their personal data in certain circumstances. This right arises in the following circumstances:

- If an individual disputes the accuracy of personal data then processing of that personal data should be restricted whilst we are verifying the accuracy of the personal data.
- If an individual has raised an objection to processing then processing should be restricted while we consider whether the objection should be upheld.
- If processing of personal data is unlawful and the individual opposes erasure and requests restriction instead.
- If the personal data is no longer required by us but the individual requires the personal data to be retained to establish, exercise or defend a legal claim.

7.2 If a request to restrict processing is made then it will be necessary for us to determine whether the request should be upheld and whether procedures need to be put in place to restrict use of the relevant personal data. If the request to restrict processing is not upheld then the individual needs to be notified of the reasons for this.

7.3 If you receive a request to restrict processing and you are concerned it goes beyond a business as usual request or are unable to confirm the identity of the individual making the request you must contact the Data Protection team immediately.

8 Right to data portability

8.1 In certain circumstances individuals can request to receive a copy of their personal data in a commonly used electronic format. This right only applies to personal data that individuals have provided to us (for example by completing a form or providing personal data through a website), or personal data that has been gathered by monitoring their behaviour. However, any analysis done by us in relation to an individual would not constitute personal data that they have provided to us and therefore is not subject to the right of data portability.

8.2 The right to data portability only applies if the processing that we are carrying out is based on the individual's consent or if the personal data must be processed for the performance of a contract. In addition, the right only applies in relation to data processing that is carried out by automated means (i.e. electronically).

8.3 In order to provide the personal data in response to a portability request the personal data must be provided in a commonly used and machine readable form.

8.4 The individual also has a right to request that the personal data is transferred directly to another organisation. If this is technically feasible then we must comply with such a request.

8.5 If you receive a data portability and you are concerned it goes beyond a business as usual request or are unable to confirm the identity of the individual making the request you must contact the Data Protection Team immediately.

9 Right to object

9.1 Individuals have a right to object to data processing being carried out by us in the following circumstances:

- If we are processing personal data based on legitimate interests or for the performance of a task in the public interest (including profiling).
- If we are using personal data for direct marketing purposes.
- If personal data is being processed for scientific or historical research or statistical purposes.

9.2 If an objection is raised in relation to personal data that is being processed on a legitimate interest or public interest ground then a balancing test must be carried out to consider whether there are any compelling legitimate grounds which enables us to continue processing the personal data. In each case the outcome of this decision and the reasons for it must be documented.

9.3 If an objection is raised in relation to direct marketing then the objection must be upheld and no balancing test will be carried out.

9.4 Individuals must be informed that they have a right to object at the point of data collection and the right to object must be explicitly brought to the attention of the individual and be presented clearly and separately from any other information.

9.5 If you receive an objection to marketing you must ensure that the relevant individual is flagged as an "opt-out" on all relevant databases immediately. If you receive an objection to other data processing activities and you are concerned it goes beyond a business as usual request or are unable to confirm the identity of the individual making the request you must contact the Data Protection Team immediately.

10 Rights related to automated decision making

10.1 Individuals have a right not to be subject to a decision which is based on automated processing where the decision will produce a legal effect or a similarly significant effect on the individual. Such decisions would include a decision whether to enter into a contract with an individual, decisions in relation to whether credit will be extended to an individual and decisions to cut off a supply.

10.2 There are exemptions from this right if the decision is necessary to enter into or perform a contract with the individual, is authorised by law or is based on explicit consent.

10.3 If one of these exemptions applies then it is still necessary to inform the individual of the automated decision making and provide them with an opportunity to object and request manual intervention.

10.4 If any automated decisions are being made then it will be necessary for us to analyse whether the decision has a legal effect or a similarly significant effect.

10.5 Where automated decisions are being made if a request for manual intervention is received, and you are concerned it goes beyond a business as usual request or are unable to confirm the identity of the individual making the request you must contact the Data Protection Team immediately.

11 Receiving and recognising requests

11.1 It is very important that all Ashford employees, contractors and councillors are aware of how to recognise a data subject request so that Ashford can comply with its obligations under the legislation.

11.2 There is no requirement for a request to be in a particular format, nor for it to be sent to any particular person within an organisation. Ashford do have an online form that we direct people to complete via the website, but if we receive a separate request, we cannot refuse to respond on the basis that the form has not been completed.

11.3 A request does not have to state that it is a request, reference any data protection legislation or even refer to “personal data” in order to be valid.

11.4 If you are unsure about whether correspondence you have received is a request relating to the personal data of a data subject, please contact The Data Protection Team immediately so that it can be reviewed.

12 What to do if you receive a request

12.1 If you receive a request, or a communication which you think might be related to the individual rights of a data subject, you should forward this to the Data Protection Team immediately together with any information you know about the background to the request.

12.2 If you receive a telephone request for information about an individual, you should:

- take steps to verify the individual's identity on the phone and not disclose any personal data about the individual unless you are sure of the caller's identity;
- refer the call to your line manager if you are not sure how to deal with the request.

12.3 We are also entitled to ask for any further information that we require to enable us to respond to the request. For example, if it is not clear from the individual's request whether he or she is requesting all information held or only some specific information. This can help us to narrow down the request (although we can't use this to restrict the scope if the data subject doesn't want to).

13 Verification of identity prior to taking any action in relation to a request

13.1 We must be satisfied that the individual making the request is in fact the individual about whom the personal data relates. If we have an ongoing relationship with the individual and have no reason to doubt the validity of a request then there is no need to take further steps. For example, if an employee or contractor makes a request using their known employment email address then no further steps to verify identity would be required. However, if a customer made a request and asked for personal data to be sent to an address that was not known to us then additional steps should be taken to verify the identity of the individuals.

13.2 Ashford may require a certified copy of the individual's photographic ID (such as a passport or driving licence) and in certain circumstances may require further identification, for example if:

- a request is being made by a third party on behalf of the data subject (see section 14 below);
- the request is made by someone whose name or details we do not recognise; or
- contact details provided in the request do not match the contact details we hold on file for the data subject.

14 Third party requests

14.1 Sometimes data subjects will ask a third party, such as a solicitor, family member or friend, to make a request on their behalf. There are certain steps

that we should take to make sure that we can disclose the relevant information to the third party.

- We may need to request further identification documents from the individual in this situation to ensure that we are confident that the individual requesting the third party to act on his/her behalf is the data subject.
- We will need to make sure we have a document authorising us to send the data subject's personal data to the third party, for example a power of attorney or letter of authority. We may also require this if two or more data subjects make a joint request.

15 Can we charge a fee?

15.1 In most cases it is not possible for us to charge a fee to comply with requests made by individuals. However, if any request is manifestly unfounded or excessive, in particular it is a repeat request, then we may charge a reasonable fee taking into account the administrative costs of providing the information or taking the action required. Alternatively in these circumstances we may refuse to act on the request. In each case we will have to be able to demonstrate that the request is manifestly unfounded or excessive and must document the reasons for this decision. This exemption may only be relied on in exceptional circumstances and if you wish to refuse a request on these grounds the decision should be escalated to the Data Protection Team to be authorised.

16 Time frames for responding to requests

16.1 In relation to the right to be informed, information must be provided at the point of data collection where personal data is collected directly from an individual. Where personal data is collected from a third party then information must be provided within one month at the latest.

16.2 In relation to all other rights we must respond without undue delay and in any event within one month. In exceptional cases this one month period may be extended by two further months if the request is particularly complex and involves a large number of requests. If we wish to make use of this extension then the individual must be informed within the initial one month period and the reasons for the delay must be explained. The ability to extend the one month period is only likely to arise in exceptional cases. If you wish to extend the period for responding to a request you must consult with the Data Protection Team .

17 Sending responses to requests

17.1 It is important to remember that responses to individual rights requests will likely contain within them personal data, often sensitive personal data. As such responses must be sent with consideration given to appropriate protection. This could include sending response by 'signed for' mail to pre-approved addresses

or password protecting content sent by emails, utilising a password that would already be known to the requester.

18 What happens if we fail to comply with a request?

18.1 Failure to comply with individuals requests under the UK GDPR are considered to be serious breaches of an individual's rights. Such breaches can in the most extreme cases attract the maximum possible fine under the UK GDPR regime. Failure to comply could also have an adverse effect on the individual. It is therefore important that all requests are recognised and are acted on promptly to enable us to respond to requests correctly and within the one month time frame.

19 Making a request

19.1 If you would like to make a request relating to your personal data, please send your written request to the Data Protection Team or complete our online form.

20 Policy updates

20.1 We will review this policy periodically and will make any updates deemed necessary. You will be required to comply with any updates made as from the date the updated policy is made available to employees.

20.2 This policy is dated [December 2022].

Ashford Borough Council

Data Security Breach Management Policy

1 Introduction

1.1 If a data security breach occurs this can have serious implications for Ashford Borough Council (referred to in this Policy as **Ashford**, **we, us or our**) and any individuals whose Personal Data may have been lost or accessed in an unauthorised manner.

1.2 This Data Security Breach Management Policy (**Policy**) explains the procedure that you should follow as soon as you become aware of a data security breach.

1.3 This Policy will help us ensure that the consequences of data security breaches are managed as quickly and effectively as possible and ensure compliance with our legal obligations, which may involve reporting data security breaches to the Information Commissioner and/or to affected individuals.

1.4 This Policy sets out the procedure which all Ashford employees and contractors (referred to in the remainder of this Policy collectively as **employees**) and all councillors must comply with if they become aware of a data security breach.

1.5 If you have any questions about this Policy, please raise them with the Data Protection team, at any of the contact details below:

Email: FOI@ashford.gov.uk
Address: Civic Centre, Tannery Lane, Ashford, Kent TN23 1PL

2 What is a data security breach?

2.1 A data security breach occurs if there is breach of security that leads to:

2.1.1 the accidental or unlawful destruction, loss or alteration of Personal Data; or

2.1.2 any unauthorised disclosure of or access to Personal Data.

2.2 For the purposes of this Policy, **Personal Data** includes information that is confidential to Ashford such as draft reports and legal advice and all personal information.

2.3 **Personal Data** includes any information about a colleague, a tenant, a member of the public or any other individual, including name, address, telephone number, bank details, health records and personnel records.

2.4 Examples of data security breaches include:

2.4.1 loss or theft of Personal Data or equipment on which Personal Data is stored;

2.4.2 inappropriate access or security controls allowing unauthorised use;

2.4.3 equipment or technical failure leading to loss of or corruption of Personal Data;

2.4.4 human error, for example sending an email to an incorrect recipient or forgetting to use the 'BCC' field instead of the 'CC' field;

2.4.5 hacking attack; or

2.4.6 "Blagging" offences where Personal Data is obtained by deceiving the organisation who holds it into believing the person requesting the information is entitled to access to the Personal Data.

2.5 A personal data breach can have serious consequences for the individuals concerned such as identity theft and fraud and it is important that each and every one of us takes responsibility for any potential, suspected, threatened or actual security breaches.

3 What do you do if there is a data security breach?

3.1 You must report **immediately** any potential, suspected, threatened or actual security breach to the Data Protection Team , who will ascertain the nature and severity of the breach.

3.2 You can use our Data Breach Reporting Form to report the breach. The Data Breach Reporting Form is available here. Please make sure you complete as much detail as possible before submitting the form to the Data Protection Team.

3.3 Your report should include the following details:

3.3.1 your name, job title and telephone and email contact details;

3.3.2 a description of what has happened;

3.3.3 when the breach occurred;

3.3.4 the volume of Personal Data involved and number of individuals affected;

3.3.5 the type(s) of data involved, including Personal Data and which individuals this affects;

3.3.6 status of the security breach, i.e. (i) potential (ii) suspected (iii) threatened (iv) actual (and if actual, has this been isolated (and how) or is it ongoing?);

3.3.7 whether the data security breach relates to a supplier arrangement and, if so, from where the security breach originated (i.e. from us or the supplier);

3.3.8 who is aware of the breach;

3.3.9 what actions have been taken to address the breach and have these mitigated any adverse effects;

3.3.10 any impacts caused as a result of the breach; and

3.3.11 any other relevant information.

4 Breach management procedure

4.1 The Data Protection Team will be responsible for co-ordinating the response to data security breaches with, where necessary, the support of the Breach Management Team. The Breach Management Team will vary depending upon the breach but may include representatives from the effected service as well as other services including Finance; HR, Communications, IT ; Legal; Policy and Performance; Customer Services; and the councils Management Team.

4.2 The Breach Management Team shall:

4.2.1 investigate the reported breach to establish the scale and nature of the breach;

4.2.2 consider what can be done to recover the loss of Personal Data;

4.2.3 identify the safeguards in place, or to be put in place, to protect the misuse of the Personal Data;

4.2.4 identify any relevant departments to assist and if appropriate, any third parties, such as banks, websites, insurers, police or credit card companies to prevent fraudulent use of Personal Data;

4.2.5 if the data security breach relates to supplier agreement, liaise with the relevant supplier in accordance with the terms of the relevant agreement;

4.2.6 by establishing the cause, determine whether any further actions can be taken to contain the breach e.g. taking systems offline, changing access codes, finding lost equipment etc.;

4.2.7 where the breach relates to unauthorised access or disclosure, determine the value of the Personal Data to the third party in receipt; and

4.2.8 take all necessary steps to mitigate the effects of the Personal Data breach.

4.3 The Data Protection Team will act as a contact point for the council and the affected individuals, and lead the co-ordination of remedial action.

5 Breach reporting

5.1 In some circumstances it will be necessary to report data security breaches involving Personal Data, to the Information Commissioner. It may also be necessary to notify individuals of a data security breach if the personal data is particularly sensitive or if individuals need to take steps to protect themselves against potential misuse of their Personal Data.

5.2 The Data Protection Team shall be responsible for determining whether a data security breach needs to be reported to regulators, including but not limited to, the Information Commissioner or whether affected individuals need to be notified.

5.3 In order to evaluate whether a data security breach needs to be reported to the Information Commissioner or whether individuals need to be notified of the breach, the Data Protection Team shall take account of all relevant regulatory guidance and shall evaluate the likely risk to individuals. The Data Protection Team should consider factors including the number of individuals affected, the nature of the Personal Data affected, including whether special categories of personal data were affected and the volume of Personal Data affected. When carrying out this evaluation consideration should be given to any risks of:

5.3.1 identity theft or fraud;

5.3.2 financial loss;

5.3.3 reputation damage;

5.3.4 loss of confidentiality protected by professional secrecy; or

5.3.5 any significant economic or social disadvantage to the individual(s) concerned.

5.4 If a data security breach involves Personal Data that is being processed by Ashford on behalf of a third party, details of the data security breach may need to be notified to that third party. The Data Protection Team shall be responsible for determining which data security breaches need to be notified to third parties.

5.5 Where we conclude that a data security breach needs to be reported to the Information Commissioner, the notification shall include the following:

5.5.1 a description of the nature of the data security breach including the categories and approximate number of data subjects and personal data records concerned;

5.5.2 details including the name and contact details of the point of contact where more information can be collected;

5.5.3 a description of the likely consequences of the data security breach; and

5.5.4 a description of the steps taken or proposed to be taken to address the data security breach and to mitigate any potential risks.

5.6 If we conclude that it is necessary to communicate the data security breach to the affected individuals, we will contact the individuals as soon as practicable. The notification will include the information noted above at 5.5.2-5.5.4 and provide individuals with advice on the steps that they can take to protect their position (if applicable).

5.7 Please note that should the Data Protection Team determine that it is necessary to notify the Information Commissioner of the data security breach, **the**

notification must take place within 72 hours of anyone within Ashford becoming aware of the breach. Therefore, it is imperative that you follow through the process in the policy **immediately**.

6 Post breach review

6.1 After the event of a data security breach and depending upon the severity of the incident the Data Protection Team and Breach Management Team shall evaluate the data security breach and the response to the breach and may prepare a report for the councils Management Team . The report shall:

6.1.1 summarise the data security breach event;

6.1.2 outline the steps taken in accordance with this Policy;

6.1.3 describe the effects of the data security breach;

6.1.4 detail the measures taken by the business to prevent similar breaches happening again; and

6.1.5 set out recommendation for any additional preventative steps that can be taken, including measures to improve the breach management response.

6.2 The Management Team shall consider the content of the post breach report and shall determine what (if any) additional steps should be taken.

6.3 Additionally all data security issues are summarised within the 6 monthly Data Protection update presented to Management Team allowing for any learning to be communicated.

7 Data security breach log

7.1 The Data Protection Team shall record details of all reported data security breaches in a data security breach log. The log must include details of the nature of the data security breach, an assessment of the severity of the breach and the potential impact on individuals, whether the breach has been reported to the regulators (and if not, the reasons why it is not necessary to report to the regulators) and the current status of the breach.

8 Policy updates

8.1 We will review this Policy periodically and will make any updates it deems necessary. You will be required to comply with any updates made as from the date the updated Policy is made available to employees. We will let you know if and when any updates are made.

8.2 This Policy was last updated on December 2022.

Ashford Borough Council
Data Security Breach Reporting Form

Please complete this form with as much information as possible, although some questions may not be relevant depending on the particular breach.

Please return the completed form to the Data Protection team

1. Details of the breach

(a) Describe the incident in as much detail as possible

(b) Is the incident (i) potential, (ii) suspected, (iii) threatened, or (iv) actual? If the breach is actual, has it been stopped or is it ongoing?

(c) How did you become aware of the breach?

(d) When did the incident happen?

(e) How did the incident happen?

(f) What type of incident was it?

(g) Which staff were involved?

(h) If the incident happened as a result of an unauthorised disclosure, have the individual responsible and the recipient of the data been identified?

(i) If there has been a delay in reporting the incident please explain your reasons for this

(j) What measures were in place to prevent an incident of this nature occurring?

(k) What policies, procedures and guidance are relevant to this incident?

(l) Were any third parties involved in this breach? [1]

2. Data placed at risk

(a) What data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent

(b) How many individuals have been affected?

[1] For example suppliers processing data on our behalf

(c) Are the affected individuals aware that the incident has occurred? If so, how did they become aware?

(d) What are the potential consequences and adverse effects on those individuals?

(e) What are the potential consequences and adverse effects on the Council?

(f) Have any affected individuals complained about the incident?

3. Containment and recovery

(a) Has any action been taken to minimise/mitigate the effect on the affected individuals?

(b) Has any action been taken to minimise/mitigate the effect on the Council?

(c) Is any future action planned?

(d) Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(e) What steps have been taken to prevent a recurrence of this incident?

4. Training and guidance

(a) Had the staff members involved in this incident received training? If so, what training and when?

(b) Is any additional training or guidance needed?

5. Reporting

(a) Who else within the Council is aware of the incident?

(b) Should the incident be reported to the police or anyone else?

(c) Has there been any media coverage of the incident?

(d) Are any other external parties aware of the breach?

6. Any other information

Form completed by:

Date:

For completion by The Data Protection Team

Log reference:

Incident types:

Data sent by email to incorrect recipient
Failure to use bcc when sending email
Data posted or faxed to incorrect recipient
Loss or theft of paperwork
Loss or theft of unencrypted device
Data left in insecure location
Cyber incident (e.g. inadvertent publication on website, phishing)
Failure to redact data
Insecure disposal of paperwork or hardware
Other

Ashford Borough Council

Data Protection Impact Assessment

Data Protection Impact Assessment Template

Project Name:	Approved by:
Author:	Date:

Data protection impact assessments (DPIAs) are tools which can help Ashford Borough Council (ABC) 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 under the UK General Data Protection Regulation (UK GDPR) whenever a 'process is likely to result in a high risk to the rights and freedoms of natural persons'.

Overview

Explain what the project aims to achieve, what the benefits will be to ABC, to individuals and to other parties and what type of data processing it involves.

Step 1. Data Protection Impact Assessment Screening Questions

These questions are intended to help ABC decide whether a full DPIA is required. If the answer is yes to any of the questions a DPIA will be required.

Will the project involve the collection of new data about individuals?	
Will the project compel individuals to provide data about themselves?	
Will data about individuals be disclosed to other organisations not previously privy to the data?	
Will data about the individuals be used for purposes it is not currently used for?	
Does the project involve new technology that might be perceived as being privacy intrusive?	
Will the project result in making decisions or taking action against individuals in ways which could have a significant impact on them?	
Is the data about individuals of a kind particularly likely to raise concerns e.g. health records, criminal records - which may be considered private?	
Will the project require contact to individuals in ways they may find intrusive?	

If yes has been answered to any of the questions above – the below full DPIA below requires completing.

Step 2. Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel, or utilises untested systems or software in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3. Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within the Council? (Data Protection Team/ Legal/IT/Etc.) Do you need to ask your data processors to assist?

Step 4. Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5. Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6. Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	**Low medium high**	**Yes/no**

Step 7 Sign off

Item	Name/position/date	Notes
Measures approved by:		***Integrate actions back into project plan, with date and responsibility for completion***
Residual risks approved by:		***If accepting any residual high risk, consult the ICO before going ahead***
Summary of DPO advice:		
DPO advice accepted or overruled by:		**If overruled, you must explain your reasons**

Ashford Borough Council

Data Sharing Protocol

1 Introduction

1.1 Ashford Borough Council (**Ashford**, **we** or **us**) sometimes receives requests from third parties for copies of personal data about our customers, employees, contractors, members of the public or other individuals. For example, we might receive requests from the police, solicitors, HMRC, councils, regulators, or even from other individuals.

1.2 We have statutory obligations in respect of disclosing personal data to third parties and we must think about whether or not we have the right or permission to disclose this Personal Data. If we breach those obligations, we could face enforcement action such as fines, claims for compensation from individuals affected and reputational damage. Therefore it is important that we are very careful about what Personal Data we send to third parties and why.

2 Purpose of this document

2.1 This Data Sharing Protocol sets out how you should treat requests received from third parties for copies of someone's personal data. Please also refer to our Data Protection Policy, which contains more information about what personal data is and how you should handle it. If you receive a request from an individual for his or her own data, please refer to our Individual Rights Policy.

2.2 This Protocol is intended to apply to one-off requests for information. If you have received a request from a third party to enter into an ongoing data sharing arrangement, please refer this to the Data Protection Team.

2.3 If you are not sure how to handle a request, please speak to your line manager or the Data Protection Team.

3 Sharing personal data

3.1 "Sharing" personal data means providing or disclosing data in any form or by any means, including telling somebody orally over the phone or in person; sending information by email, text or other online messaging service; enabling access to electronic information (for example through an internet portal); and providing information in hardcopy form.

3.2 Personal data held by Ashford must only be shared in accordance with this Protocol or a data sharing agreement or when released under a request under the Freedom of Information Act or the Environmental Information Regulations (subject to the data protection exemptions or exceptions).

4 General principle

4.1 Our starting point should always be that personal data should not be disclosed to anyone who the information is not about. Personal data is private to the individual to whom it relates and often individuals would not expect us to provide personal data about them to other people without their consent.

5 Sharing for limited purposes

5.1 We may be able to share personal data with third parties if:

5.1.1 the sharing is for purposes that we have told the individual about; and

5.1.2 we have told the individual that their data will be shared, or the individual would reasonably expect their data to be shared for these purposes.

5.2 For example, we may need to share personal data with our pension provider to enable our employees' pensions to be administered. We are allowed to do this provided we have told our employees that their data will be used for the purposes of administering pensions and other benefits, as employees would reasonably expect us to have to share data with a provider for this purpose.

5.3 In order to establish whether you can share data in this way, you should therefore look at the privacy policy or other privacy information that has been provided to the individual whose data you are proposing to share. If that information does not cover sharing for the purposes at hand, you will need to inform the individual that you are going to share their data for these purposes. Depending upon the legal basis for processing this data you may need to capture additional consents.

6 Sharing with consent

6.1 If you want to share personal data with a third party:

6.1.1 for purposes other than purposes we have already told the individual about;

6.1.2 in circumstances where the individual would not expect their Personal Data to be shared; or

6.1.3 where the data involved is sensitive personal data (for example, medical information, information about race or religion, information about political opinions or trade union membership,

you may need to obtain the consent of the individual to whom the Personal Data relates before you share the Personal Data.

6.2 When you obtain consent, you should make sure that the individual knows exactly what they are consenting to. This means giving a very clear

description of who the Personal Data will be shared with and why.

6.3 You must make sure that consent is recorded somewhere that is clear and easily accessible in our systems. This is so that if we are ever challenged on our decision to share Personal Data, we can demonstrate that appropriate consent was obtained.

6.4 Remember that individuals can withdraw consent at any time. If someone changes their mind before you share the Personal Data, you must not share it. If someone changes their mind after you share the Personal Data, you may need to take steps to retrieve the Personal Data.

7 Sharing information with councillors

7.1 We will not normally need to obtain specific consent to share personal data with councillors provided that:

7.1.1 the councillor represents the ward in which the relevant individual lives;

7.1.2 the councillor makes it clear that he or she is representing that individual in the request for personal information;

7.1.3 the personal information is necessary to respond to the individual's complaint and/or to enable the councillor to carry out his or her official duties; and

7.1.4 the information is not particularly private or sensitive.

8 Legal obligations to share Personal Data

8.1 There may be certain situations when we are under a legal obligation to share Personal Data. For example, if someone has obtained a court order or a warrant which requires us to share Personal Data, then we must do so otherwise we will be in breach of our legal obligations.

8.2 However, we must only disclose the minimum amount of Personal Data that is required by that legal obligation. For example, if a court order requires us to share someone's name and phone number, we shouldn't also share their postal address.

9 Exemptions

9.1 As well as legal obligations, there are certain exemptions that we can rely on to enable us to share personal data. These exemptions allow us to share personal data without obtaining consent and without telling the individual, as long as the data is required for certain purposes.

9.2 The main exemptions are as follows:

9.2.1 We can share Personal Data with a third party where it is necessary to do so for the purposes of preventing or detecting crime, or for apprehending or prosecuting offenders or the assessment or collection of a tax. These types of requests are likely to come from the police, other enforcement authority or another council and relate to an ongoing investigation; and

9.2.2 We can share Personal Data with a third party where it is necessary to do so for the purposes of legal proceedings, obtaining legal advice, or otherwise exercising, establishing or defending legal rights. These types of requests are likely to come from solicitors or from other third parties who are intending to take proceedings against an individual.

9.3 If you receive a request from a third party and you think it might fall under one of these exemptions, you should make sure that the request is made in writing and you should send the request to the Data Protection Team immediately. The third party requesting the data will need to tell us the reasons why the information requested is necessary for those purposes and we will need to make sure that we are satisfied that the information is, in fact, necessary. If you are not sure that the information is necessary, **you must not share the Personal Data.** You can tell the requester to obtain a court order for disclosure of the information if there is any doubt as to whether we should share the information.

10 Verification of identity

10.1 Even if you have someone's consent to share their Personal Data or there is an exemption or a legal obligation, you should always verify the identity of the person making the request so that you don't inadvertently share Personal Data with someone else.

10.1.1 **Individuals:** Other individuals may request data relating to someone else. For example, the daughter of an elderly council tenant might ask for a copy of the tenancy. You should make sure that you know who the requester is, the relationship that he or she claims to have with the person about whom information is requested and that he or she is entitled to have the information (for example, because there is a power of attorney or letter or authority in place).

10.1.2 **Authorities:** Sometimes the police or HMRC might ask us for information to assist with crime prevention or tax collection. For example, the police might ask us for the telephone number of a tenant they suspect of fraud. You should take steps to verify the identity and job title of the person, for example asking for a work email address, checking with the relevant police force or finding a generic telephone number for the authority online and contacting the requester that way.

10.1.3 **Third party companies:** If you receive a request from a third party company or another local authority, for example because the individual has applied for a job there and the request is for a

reference, you should verify that the company exists and that the person making the request works there and has the job title he/she says he/she has.

11 Minimisation of Personal Data

11.1 Even where a decision is taken to share personal data with a third party, we must always remember that we have an obligation to make sure that the minimum amount of personal data necessary is processed, which includes sharing with third parties. Therefore, you should only disclose the minimum amount of Personal Data that is necessary for our or the third party's purposes.

11.2 For example, if the police request someone's telephone number as that personal is suspected of fraud and the police need to track that person, you may be able to disclose the telephone number but you should not disclose other information such as that person's address or personal details, even if you think it would be helpful to do so.

12 Transmission of Personal Data

12.1 As well as our obligations in terms of sharing personal data, we also have obligations to keep personal data secure. This means that when you share personal data with third parties, you should do so in a way that is technologically and physically secure.

12.2 If Personal Data is transmitted by electronic means, such as by email, file transfer link or portable device, the email, file or device should be password protected, or encrypted if information is sensitive or risky.

12.3 If data is provided in hardcopy, this should either be physically handed to the recipient or sent by recorded delivery and marked "confidential".

12.4 Always make sure that you send the Personal Data to the correct person. If sending electronically, check that you have put in the correct email address. If you hand the Personal Data to someone in hardcopy, check their ID and if you post hardcopy information to someone, make sure it is signed for by the right person.

13 Recording your decision

13.1 If we are ever challenged by an individual or the regulator on sharing personal data, it is important that we are able to demonstrate that the sharing was compliant with data protection laws. We must therefore make sure that there is an appropriate audit trail.

13.2 Once you have made the decision to share, or not to share, data, you must record that decision (and the rationale) in writing and in a place that is easily accessible on our systems or in our files. You should make sure that your record includes what information was shared and why, with whom, your justification for sharing it, and whether or not consent was obtained from the

relevant individual.

14 Sharing Personal Data with suppliers

14.1 If we need to share personal data with any third party suppliers who will use that Personal Data for the purposes of carrying out services on Ashford's behalf (rather than for their own purposes), we can normally do this but we must do two things to make sure that this is compliant:

14.1.1 We must conduct appropriate due diligence on the supplier or third party to assess their information security and data protection procedures before we send them any personal data. We should check that they have adequate policies and security measures in place, and that all their staff are appropriately trained on data protection.

14.1.2 We must also make sure there is a written contract in place with the supplier or third party which includes certain standard clauses governing what they can and can't do with personal data. Please make sure that you contact the Data Protection Team if you need to put a contract in place with a supplier who will process personal data on our behalf so that the Data Protection Team can make sure that the data protection clauses are adequate.

15 Kent and Medway Information Sharing Agreement

15.1 We are signatories to the Kent and Medway Information Sharing Agreement which provides a framework between which personal data may be shared with signatory organisations or public bodies across Kent and Medway, as long as there is an appropriate legal basis for the share. When sharing information with signatories you must adhere to the agreement and keep a record of the sharing that has taken place.

16 Updates to this Protocol

16.1 We will review this Protocol periodically and will make any required updates. You will be required to comply with any updates from the date the updated Protocol is made available. We will let you know when updates are made.

Last updated: December 2022

Ashford Borough Council

Data Protection Compliance Monitoring Protocol

Purpose of this document

This Data Protection Compliance Monitoring Protocol is intended to provide practical guidance to key stakeholders within Ashford Borough Council (**Ashford**) who are responsible for monitoring compliance with data protection laws across Ashford. Key stakeholders are likely to be senior members of Service Areas the Data Protection Team and/or those in executive or director roles. The terms **you**, **your** etc. throughout this Data Protection Protocol refer to those key stakeholders.

Ashford collects and uses a huge amount of personal data and has statutory obligations in respect of that personal data. Ashford has a number of data protection related policies and procedures in place, including:

- Data Protection Policy;
- Breach Management Policy;
- Individual Rights Policy;
- Data Sharing Protocol;
- Data Protection Impact Assessment template;

Ashford also provides induction and refresher training on data protection.

These policies and training help Ashford to demonstrate that it is compliant with data protection legislation. However, full compliance is not possible unless all employees are aware of the importance of the rules and are taking steps on a day-to-day basis to protect personal data.

This Protocol therefore sets out the steps that you should be taking, as key stakeholders, to ensure that your team members and other colleagues are alive to data protection issues in their day-to-day roles, and that they take on board and comply with the requirements of the legislation.

Practical tips to ensure compliance

	Lead by example
	• Make sure you are familiar with Ashford's Data Protection policies and procedures • Ensure you are taking all practical steps recommended by those policies and procedures and any additional steps required to protect personal data

	Ensure that all team members handling personal data are aware of Ashford's policies and procedures and have read and understood them
	• Discuss policies and procedures as part of initial training and ask team members to explain what their understanding is of the policies and procedures • Raise compliance with policies and procedures as part of supervision and ongoing training • Incorporate compliance with policies and procedures as part of annual appraisals

	Make sure all team members complete Ashford's induction training and annual refresher training on data protection
	• Keep a log of those team members who have completed the training and those who have not • Issue reminders to team members who have not completed the training within the required timescales • Escalate to senior management when team members have not completed the training within the required timescales

	Encourage people to "think privacy"
	• If you and/or your team members are involved in new projects involving personal data, raise data protection as a key consideration at the outset • If projects present a significant data protection risk, make sure you or your team members liaise with the Data Protection Team to establish whether further steps need to be taken to ensure data is adequately protected, for example carrying out a Data Protection Impact Assessments.

	Build a culture of data protection compliance
	• Encourage team members to build habits of thinking about personal data • For example, ask those working on new projects to explain what the data implications of projects are

	Look out for day-to-day compliance
	• Regularly review what your team members and colleagues are doing with personal data • For example, are individuals locking paper files away, locking their screens when away from their desks, password-protecting sensitive files? • If certain individuals are regularly failing to take steps like this to protect personal data, consider whether there are additional training needs for those individuals or whether further information/guidance is required • Ensure that team members know that failure to comply with data protection requirements may become a disciplinary issue

	Carry out regular spot-checks
	• Implement regular audits and/or spot-checks among your team to test compliance with data protection requirements • If audits and spot-checks reveal gaps in compliance, identify whether there are additional training or guidance needs and address them if so • Escalate any Data Protection concerns identified a part of the spot-checks/audits to the Data Protection Team

	Be prepared to answer questions
	• Make it clear to your team that you are available if they have any questions or concerns about data protection • Be willing and able to deal with queries from team members and Colleagues

	Get to know the Data Protection Team
	• Get to know Ashford's Data Protection Team so that you feel comfortable speaking about issues and questions you or your team have • Liaise with the Data Protection Team on a regular basis and raise questions as soon as they arise

	Deal with breaches in your team effectively
	• If someone notifies you of a data breach, find out as much information as you can about the breach • Make sure breaches reported to you are escalated to the Data Protection Team immediately and in accordance with Ashford's Breach Management policy • Identify and implement additional measures and or training needs arising out of a breach

	Keep systems up to date
	• If you or your Service Area are responsible for systems used by Ashford, make sure that these systems are up-to-date • If you or your Service Area use manual filing and archiving systems, encourage a Management Policy where regular file and archive reviews are conducted to ensure that data is destroyed where necessary

	Keep the Data Protection Team informed of new uses of data
	• If your Service uses data in a new way, you should immediately inform the Data Protection Team as we may need to notify the Information Commissioner or our users to this new use of data • The Data Protection Team will also be able to assist with any necessary data protection measures to accompany this new use, for example; privacy notices, processing clauses in contracts and general good data governance.

Questions about this Protocol

If you have any queries about this Protocol or if you are not sure what you should be doing to assist and ensure compliance, please contact the Data Protection Team.

Last updated: December 2022