Appendix C

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 our data protection officer (**DPO**), Charlotte Hammersley, at the following contact details:

Email:	charlotte.hammersley@ashford.gov.uk
Phone:	01233 330878
Address:	Civic Centre, Tannery Lane, Ashford, Kent, TN23 1PL

2 Definitions

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

2.1.1 **data controller**: this means the entity which determines how, and for what purposes, personal data will be collected and used. Ashford is a data controller and has an obligation to comply with data protection legislation;

2.1.2 **data subject**: this means the individual to whom personal data relates;

2.1.3 **personal data (or personal information)**: this means any information about a living individual (including customers, employees, suppliers and contractors of Ashford) who can be identified from that information, or from that information together with other information held by Ashford or third parties. Personal data may include things like customer application forms and contact details; employee files; call recordings and CCTV footage and correspondence with a customer or another individual;

2.1.4 **processing**: this means any operation performed on the personal data, including, organising, retrieving, using, disclosing and simply holding information.

3 What rights do individuals have under data protection legislation?

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

3.1.1 the right to be informed;

3.1.2 the right of access;

3.1.3 the right to rectification;

3.1.4 the right to erase;

3.1.5 the right to restrict processing;

3.1.6 the right to data portability;

3.1.7 the right to object;

3.1.8 rights in relation to automated decision making and profiling.

3.2 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.

4 The right to be informed

4.1 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.

4.2 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.

4.3 The 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.

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

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

4.5.1 employee privacy notice;

4.5.2 recruitment privacy notice;

4.5.3 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;

4.5.4 task specific privacy notices.

5 Right of access – Known as a Subject Access Request

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

5.1.1 obtain confirmation of whether we are processing their personal data;

5.1.2 access their personal data; and

5.1.3 information regarding how their personal data is being used by us.

5.2 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.

5.3 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 their 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.

5.4 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.

5.5 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.

5.6 If a request for access is received you must contact the DPO immediately.

6 Right to rectification

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

6.2 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.

6.3 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.

6.4 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.

6.5 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 DPO immediately.

7 Right to erasure

7.1 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:

7.1.1 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

7.1.2 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);

7.1.3 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;*

7.1.4 if the personal data has been processed unlawfully (i.e. in breach of the requirements of the GDPR); or

7.1.5 if it is necessary to delete the personal data to comply with a legal obligation.

7.2 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 or for research purposes.

7.3 If you receive a request to erase personal data you must contact the DPO immediately.

8 Right to restrict processing

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

8.1.1 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.

8.1.2 If an individual has raised an objection to processing then processing should be restricted while we consider whether the objection should be upheld.

8.1.3 If processing of personal data is unlawful and the individual opposes erasure and requests restriction instead.

8.1.4 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.

8.2 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.

8.3 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 DPO immediately.

9 Right to data portability

9.1 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 then this personal data will also be subject to the right to data portability. 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.

9.2 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).

9.3 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.

9.4 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.

9.5 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 DPO immediately.

10 Right to object

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

10.1.1 If we are processing personal data based on legitimate interests (please see paragraph 7.1.3 regarding our reliance on legitimate interests as a legal basis for processing) or for the performance of a task in the public interest (including profiling).

10.1.2 If we are using personal data for direct marketing purposes.

10.1.3 If personal data is being processed for scientific or historical research or statistical purposes.

10.2 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.

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

10.4 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.

10.5 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 DPO immediately.

11 Rights related to automated decision making

11.1 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.

11.2 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.

11.3 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.

11.4 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. If so then advice

should be sought from our in relation to the steps that need to be taken to ensure that the automated decision making is carried out in a compliant way.

11.5 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 DPO immediately.

12 Receiving and recognising requests

12.1 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.

12.2 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.

12.3 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.

12.4 If you are unsure about whether correspondence you have received is a request relating to the personal data of a data subject, please contact Ashford's data protection officer (**DPO**) immediately so that it can be reviewed.

13 What to do if you receive a request

13.1 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 DPO immediately together with any information you know about the background to the request.

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

13.2.1 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;

13.2.2 refer the call to your line manager if you are not sure how to deal with the request.

13.3 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).

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

14.1 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.

14.2 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:

14.2.1 a request is being made by a third party on behalf of the data subject (see section 15 below);

14.2.2 the request is made by someone whose name or details we do not recognise; or

14.2.3 contact details provided in the request do not match the contact details we hold on file for the data subject.

15 Third party requests

15.1 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.

15.1.1 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.

15.1.2 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.

16 Can we charge a fee?

16.1 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 our to be authorised.

17 Time frames for responding to requests

17.1 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. Please see section 3.2 above for more information.

17.2 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 our.

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

18.1 Failure to comply with individuals requests under the GDPR are considered to be serious breaches of an individual's rights. Such breaches can attract the maximum

possible fine under the GDPR regime, which equates to up to a 4% of Group turnover or €20million. 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 your personal data, please send your written request to the DPO.

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 [24 May 2018].