THE FINANCE CARE SERVICE
"A Helping Hand"

DATA PROTECTION STATEMENT (GDPR POLICY)

4th January 2021

1. Introduction This Policy sets out the obligations of the Finance Care Service ("the Company") regarding data protection and the rights of individuals ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation"). The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a 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. This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company. The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be: o processed lawfully, fairly, and in a transparent manner in relation to the data subject; o collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; o adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; o 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 they are processed, is erased or rectified without delay; o kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject; o 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.

3. Lawful, Fair, and Transparent Data Processing The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies: o the data subject has given consent information to the processing of his or her personal data for one or more specific purposes; o processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; o processing is necessary for compliance with a legal obligation to which the controller is subject; o processing is necessary to protect the

vital interests of the data subject or of another natural person; o 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 controller; o processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. Processed for Specified, Explicit and Legitimate Purposes The Company collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, information received from local authorities and other statutory organisations). The Company only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. Adequate, Relevant and Limited Data Processing The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up To Date The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Timely Processing The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. Secure Processing The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this policy

9. Accountability The Company's data protection / privacy officer is Daniel Slaven. The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information: The name and details of the Company, its data protection officer, and any applicable third party data controllers; The purposes for which the Company processes personal data; Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates; Details (and categories) of any third parties that will receive personal data from the Company; Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards; Details of how long personal data will be retained by the Company; and Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

10. Privacy Impact Assessments The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance: The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data; Details of the legitimate interests being pursued by the Company; An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed; An assessment of the risks posed to individual data subjects; and Details of the measures in place to minimise and handle risks including safeguards, data security,

and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. The Rights of Data Subjects The Regulation sets out the following rights applicable to data subjects: The right to be informed; The right of access; The right to rectification; The right to erasure (also known as the 'right to be forgotten'); The right to restrict processing; The right to data portability; The right to object; Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed The Company shall ensure that the following information is provided to every data subject when personal data is collected: Details of the Company including, but not limited to, the identity of Daniel Slaven, its Data Protection Officer; The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing; Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data; Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed; Where the personal data is to be transferred to one or more third parties, details of those parties; Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers); Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined); Details of the data subject's rights under the Regulation; Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time; Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation); Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences. The information set out above shall be provided to the data subject at the following applicable time: Where the personal data is obtained from the data subject directly, at the time of collection; Where the personal data is not obtained from the data subject directly (i.e. from another party): i. If the personal data is used to communicate with the data subject, at the time of the first communication; or ii. If the personal data is to be disclosed to another party, before the personal data is disclosed; or iii. In any event, not more than one month after the time at which the Company obtains the personal data.

13. Data Subject Access A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension). All subject access requests received must be forwarded to Daniel Slaven, the Company's data protection officer contactable as follows: Daniel Slaven, Data Protection Controller, Finance Care Service, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ. The Company charges at fee of £10 for standard handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject

shall be informed of the need for the extension). In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. Erasure of Personal Data Data subjects may request that the Company erases the personal data it holds about them in the following circumstances: It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed; The data subject wishes to withdraw their consent to the Company holding and processing their personal data; The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object); The personal data has been processed unlawfully; The personal data needs to be erased in order for the Company to comply with a particular legal obligation; Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension). In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations). Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller. All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).]

18. Objections to Personal Data Processing Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes. Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith. Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making In the event that the Company uses personal data for the purposes of automated decisionmaking and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company. The right described above does not apply in the following circumstances: The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject; The decision is authorised by law; or The data subject has given their explicit consent.

20. Profiling Where the Company uses personal data for profiling purposes, the following shall apply: Clear information explaining the profiling will be provided, including its significance and the likely consequences; Appropriate mathematical or statistical procedures will be used; Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

21. Personal Data The following personal data may be collected, held, and processed by the Company: Name, date of birth, national insurance and contact details of the data subject. This is so we are able to contact you in order to carry out the services we are retained to deliver and to maintain up to date information records.; Financial information and related records. We require such information as we would not be able to perform the services that we are retained to deliver without this data; Certain restricted medical records and information. Medical information particularly around mental capacity assessments are required in order for us to undertake the services we are retained to deliver. Information about the data subject's family or care support contacts and other professional contacts involved in supporting the data subject with their needs. We require such information in order to deliver the services that we are asked to provide; Additional ad hoc information that is required for us to provide the services we are retained to deliver.

22. Data Protection Measures The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data: All emails containing personal data of a sensitive nature will to be best of our abilities be encrypted using a Secure Email System; Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely are retained confidential waste disposal service (currently provided by Shred-It) Sensitive personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances; Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable; Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data; Where sensitive personal data is to be transferred in hardcopy form it should be passed directly to the recipient or or sent using the Royal Mail Recorded Delivery Service or another secure postal carrier service.; No personal data may be shared informally and if an employee, agent, subcontractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Controller or another individual authorised by the Data Controller. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar; No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Data Controller or another individual authorised by the Data Controller. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time; If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; No personal

data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise the Data Controller or another individual authorised by the Data Controller and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken) All electronic copies of personal data should be stored securely using passwords and accessible only to those authorised personnel who have a requirement to access the data. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. Personal data will not be used to undertake third party marketing activities.

23. Organisational Measures The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data: o All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy; Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company; All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so; All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised; Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed; The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed; All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract; All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation; Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. **Data Breach Notification** All personal data breaches must be reported immediately to the Company's data protection officer. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay. Data breach notifications shall include the following information: The categories and approximate number of data subjects

concerned; The categories and approximate number of personal data records concerned; The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained); The likely consequences of the breach; Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

25. **Implementation of Policy** This Policy shall be deemed effective as of 4th December 2019. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by the Finance Care Service on 4th December 2019.

THE FINANCE CARE SERVICE
"A Helping Hand"

THE FINANCE CARE SERVICE
"A Helping Hand"

WEBSITE PRIVACY NOTICE

This policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it. By visiting our website you are accepting and consenting to the practices described in this policy.

For the purpose of the Data Protection Act 1998 (the Act) and, the data controller is Daniel Slaven, Finance Care Service, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ.

Data protection law has changed in the UK with the Data Protection Act 1998 ('DPA') being replaced with the European General Data Protection Regulation ('GDPR') form 25 May 2018.

This Privacy Statement explains how we process your information and your rights under both DPA and GDPR.

Information we may collect from you

We may collect and process the following data about you:

1. **Information you give us.** This could be your name, date of birth and telephone and/or email contact details along with a description of why you have contacted us via our website.
2. **Information we receive from other sources.** Other sources could be social workers or other representatives of a local authority, medical professionals, advocates or care organisations for example. They may provide your name, date of birth and contact details along with a description of why they have chosen to contact us via our website on your behalf.

Cookies

Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site. For detailed information on the cookies we use and the purposes for which we use them see our Cookie Policy below.

Uses made of the information

We use information held about you in the following ways:

1. **Information you give to us.** We will use this information to make contact with you if possible, in order to ascertain how we may be of assistance to you.

2. **Information we receive from other sources.** We may combine this information with information you give to us and information we collect about you. We may us this information and the combined information for the purposes set out above (depending on the types of information we receive).

Disclosure of your information

We may share your personal information with:

- Employees of The Company in order to undertake the services we have been retained to provide on your behalf**.**

We may share your information with selected third parties including:

- Business partners, suppliers and sub-contractors for the performance of any contract we enter into with [them or] you, including without limitation any data processor we engage. Examples of such third parties are: The Department of Work and Pensions (DWP), approved independent social workers, approved genealogy organisations, law firms, analytics and search engine providers that assist us in the improvement and optimisation of our site.

We may disclose your personal information to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our Terms of Use or terms and conditions of supply and other agreements; or to protect the rights, property, or safety of Finance Care Service, our Clients, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

Where we store your personal data

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff maybe engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy.

All information you provide to us is stored on our secure servers. Any payment transactions will be encrypted using SSL technology. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Your rights

You have the right to ask us not to process your personal data for marketing purposes. We will inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your data. You can also exercise the right at any time by contacting us at info@financecareservice.org.

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Your rights under Data Protection Law

We operate under the Data Protection Act 1998 ('DPA') as replaced by the European General Data Protection Regulation ('GDPR') from 25 May 2018.

The DPA and GDPR apply to 'personal data' we process and the data protection principles set out the main responsibilities we are responsible for.

We must ensure that personal data shall be:

- ✓ processed lawfully, fairly and in a transparent manner;
- ✓ collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- ✓ adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- ✓ accurate and where necessary kept up to date;
- ✓ kept for no longer than is necessary for the purposes for which the personal data are processed. We operate a data retention policy that ensures we meet this obligation.
- ✓ only retain personal data for the purposes for which it was collected and for a reasonable period thereafter where there is a legitimate business need or legal obligation to do so. For detail of our current retention policy contact our privacy officer at info@financecareservice.org.uk
- ✓ 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.

We ensure lawful processing of personal data by obtaining consent; or where there is a contractual obligation to do so in providing appropriate products and services; or where processing the data is necessary for the purposes of our legitimate interests in providing appropriate products and services.

In the majority of cases we process personal data based on your contract with us. In other cases, we process personal data only where there are legitimate grounds for so doing.

To meet our Data Protection obligations, we have established comprehensive and proportionate governance measures.

We ensure data protection compliance across the organisation through:

- ✓ implementing appropriate technical and organisational measures including internal data protection policies, staff training, internal audits of processing activities, and reviews of internal HR policies.
- ✓ maintaining relevant documentation on processing activities.
- ✓ implementing measures that meet the principles of data protection by design and data protection by default including data minimisation, pseudonymisation, transparency, deploying the most up-to-date data security protocols and using data protection impact assessments across our organisation and in any third party arrangements.

How you can obtain a copy of the data we hold about you

You have a right to receive a copy of the personal data that we hold about you. Under the DPA We have the discretion to make a charge of £10.00 towards the cost of administration

To obtain a copy of the personal information we hold on you, please write to us at the address below and provide us with your details or ask for a Subject Access Request form.

Under the DPA you also have a number of additional rights in respect of your personal data. The Information Commissioner's website provides guidance on these at www.ico.org.uk

Questions regarding this Privacy Statement should be directed to:

The Data Controller, Finance Care Service, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ

From 25 May 2018 under the GDPR You have the following specific rights in respect of the personal data we process:

1. The right to be informed about how we use personal data. This Privacy Statement explains who we are; the purposes for which we process personal data and our legitimate interests in so doing; the categories of data we process; third party disclosures; and details of any transfers of personal data outside the UK.
2. The right of access to the personal data we hold. In most cases this will be free of charge and must be provided within one month of receipt.
3. The right to rectification where data are inaccurate or incomplete. In such cases we shall make any amendments or additions within one month of your request.

4. The right to erasure of personal data, but only in very specific circumstances, typically where the personal data are no longer necessary in relation to the purpose for which it was originally collected or processed; or, in certain cases where we have relied on consent to process the data, when that consent is withdrawn and there is no other legitimate reason for continuing to process that data; or when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
5. The right to restrict processing, for example while we are reviewing the accuracy or completeness of data, or deciding on whether any request for erasure is valid. In such cases we shall continue to store the data, but not further process it until such time as we have resolved the issue.
6. The right to data portability which, subject to a number of qualifying conditions, allows individuals to obtain and reuse their personal data for their own purposes across different services.
7. The right to object in cases where processing is based on legitimate interests, where our requirement to process the data is overridden by the rights of the individual concerned; or for the purposes of direct marketing (including profiling); or for processing for purposes of scientific / historical research and statistics, unless this is for necessary for the performance of a public interest task.
8. Rights in relation to automated decision making and profiling.

Please contact our privacy officer at Info@financecareservice.org more information about the GDPR and your rights under Data Protection law.

If you have a complaint about data protection at Finance Care Service contact our privacy officer at Info@financecareservice.org

Alternatively contact our supervisory authority for data protection compliance (www.ico.org.uk):

Information Commissioner's Office
Wycliffe House
Water Lane, Wilmslow
Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 (national rate)

About cookies

Cookies are pieces of information that a website transfers to your computer's hard disk for record-keeping purposes. Cookies can make the internet more useful by storing information about your preferences on a particular site, such as your personal preference pages.

The use of cookies is an industry standard, and most websites use them to provide useful features for their customers. Cookies in and of themselves do not personally identify users, although they do identify a user's computer. Most browsers are initially set to accept cookies.

If you would prefer, you can set yours to refuse cookies. However, you may not be able to take full advantage of a website if you do so.

Changes to our privacy policy

Any changes we may make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by e-mail. Please check back frequently to see any updates or changes to our privacy policy.

Contact

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to info@financecareservice.org

Last updated: 4th January 2021

THE FINANCE CARE SERVICE
"A Helping Hand"