SUBJECT ACCESS REQUEST POLICY

1. Purpose

1.1 This document sets out our policy for responding to subject access requests under the EU General Data Protection Regulations (**GDPR**). The GDPR took effect from 25 May 2018.

1.2 The rights and responsibilities of those dealing with personal data and your rights as a data subject are contained in the GDPR. All staff are contractually bound to comply with the GDPR and other relevant policies.

2. Introduction – what is the GDPR?

2.1 The GDPR replaces and extends the previous data protection framework and has been incorporated in the UK by the Data Protection Act 2018. The GDPR gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

2.2 The GDPR states the following:

2.2.1 Firstly, anyone who processes personal information must comply with eight principles of data protection, which make sure that personal information is:

(a) fairly and lawfully processed;

(b) processed for specific and lawful purposes;

(c) adequate, relevant and not excessive;

(d) accurate and up-to-date;

(e) not kept for longer than is necessary;

(f) processed in line with the individuals' rights;

(g) secure;

(h) not transferred to other countries without adequate protection.

2.2.2 Secondly, it provides individuals with important rights, such as:

(a) the right to be informed;

(b) the right to rectification;

(c) the right to erasure;

(d) the right to restrict processing;

(e) the right to data portability;

(f) the right to object;

(g) rights related to automated decision-making, including profiling.

3. What is The Grange Trust's general policy on providing information?

We welcome the rights of access to information that are set out in the GDPR. We are committed to operating openly and to meeting all reasonable requests for information that are not subject to specific exemption in the GDPR.

4. How do you make a subject access request?

A subject access request is a request for personal information (known as personal data) held about you by us. The request can be made verbally, electronically or in writing. We recommend you use our Request Form to help us identify the data you request quickly and avoid any delays. Generally, you have the right to see what personal information we hold about you, you are entitled to be given a description of the information, what we use it for, who we might pass it on to and any information we might have about the source of the information. However, this right is subject to certain exemptions that are set out in the GDPR.

5. What is personal information?

5.1 Personal data is information which has the individual as its focus and is identifiable to the data subject.

5.2 Further information on what amounts to personal data can be found at the Appendix.

6. What do we do when we receive a subject access request?

Checking of identity

6.1 We will first check that we have enough information to be sure of your identity. Often we will have no reason to doubt a person's identity, for example, if we have regularly corresponded with them. However, if we have good cause to doubt your identity we can ask you to provide any evidence we reasonably need to confirm your identity. For example, we may ask you for a piece of information held in your records that we would expect you to know: a witnessed copy of your signature or proof of your address.

6.2 If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone under the Mental Capacity Act 2005, you must confirm your capacity to act on their behalf and explain how you are entitled to access their information. If you are the parent/guardian of a child under 16, we will need to consider whether the child can provide their consent to you acting on their behalf.

6.3 Should you make a data subject access request but you are not the data subject, you must stipulate on what legal basis you request this information and have access to it.

Collation of information

6.4 We will check that we have enough information to find the records you requested. If we feel we need more information, then we will promptly ask you for this. We will gather any manual or electronically held information (including emails) and identify any information provided by a third party or which identifies a third party. This includes records created before 25 May 2018.

6.5 If we have identified information that relates to third parties, we will write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information to you unless the other party has provided their consent or it is reasonable to do so without their consent. If the third party objects to the information being disclosed, we may seek legal advice on what action we should take.

6.6 Before sharing any information that relates to third parties, we will where possible anonymise information that identifies third parties not already known to the individual (e.g. employees), and edit information that might affect another party's privacy. We may also summarise information rather than provide a copy of the whole document. The GDPR requires us to provide information not documents.

Issuing our response

6.7 Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent to you unless otherwise agreed.

6.8 Any information supplied by us will remain the property of the Grange Trust and must not be distributed to any third party.

6.9 We will explain any complex terms or abbreviations contained within the information when it is shared with you. Unless specified otherwise, we will also provide a copy of any information that you have seen before.

7. Will we charge a fee?

Under the GDPR there is no fee payable. However, where we feel the request is 'manifestly unfound or excessive' we may charge a reasonable administrative costs fee. If more than one copy of the information is required we will also charge a reasonable administrative costs fee.

8. What is the timeframe for responding to subject access requests?

We have one month starting from when we have received all the information necessary to identity you, to identify the information requested, and any fee required, to provide you with the information or to provide an explanation about why we are unable to provide the information. We may seek an extension if the request is particularly complex.

9. Are there any grounds we can rely on for not complying with a subject access request?

Previous request

9.1 If you have made a previous subject access request we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

Exemptions

9.2 The GDPR contains a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. This includes if disclosing the information would adversely affect the rights and freedoms of others.

10. What if you identify an error in our records?

If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. We will consider informing any relevant third party of the correction. If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file.

11. What if you want us to stop processing your data?

Under section 21 of the GDPR, you can object to our processing your data altogether, in relation to a particular purpose or in a particular way through a data subject notice. However, this only applies to certain processing activities and there is a process that you must follow when making such an objection. We must then give you written notice that either we have complied with your request, intend to comply with it or state the extent to which we will comply with it and why. This information will be given to you within 21 days of receiving the data subject notice. Further information on this can be found at www.informationcommissioner.gov.uk.

12. Our complaints procedure

12.1 If you are not satisfied by our actions, you can seek recourse through our internal complaints procedure, the Information Commissioner or the courts.

12.2 Data Protection & Compliance Solutions Limited will deal with any written complaint about the way a request has been handled and about information has been disclosed they can be contacted at:

Data Protection & Compliance Solutions Limited

Number One Railway Court, Ten Pound Walk, Doncaster, DN4 5FB

Telephone: 01302 965865
Email: phil@dpcsuk.co.uk; rajinder@dpcs.co.uk

12.3 If you remain dissatisfied, you have the right to refer the matter to the Information Commissioner. The Information Commissioner can be contacted at:

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

Telephone: 01625 545745
Fax: 01625 524510
Email: enquiries@ico.gsi.gov.uk

APPENDIX

1. Personal data is information that relates to a living individual who can be identified from the information and which affects the privacy of that individual, either in a personal or professional capacity. Any expression of opinion about the individual or any indication of the intentions of any person in respect of the individual will be personal data.

2. Provided the information in question can be linked to an identifiable individual, the following are likely to be examples of personal data:

2.1 an individual's salary or other financial information;

2.2 information about an individual's family life or personal circumstances, employment, any opinion about an individual's state of mind;

2.3 sensitive personal information – an individual's racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual orientation, criminal record and membership of a trade union.

3. The following are examples of information which will not normally be personal data:

3.1 mere reference to a person's name, where the name is not associated with any other personal information;

3.2 incidental reference in the minutes of a business meeting of an individual's attendance at that meeting in an official capacity;

3.3 where an individual's name appears on a document or email indicating only that it has been sent or copied to that particular individual;

3.4 the content of that document or email does not amount to personal data about the individual unless there is other information about the individual in it.

4. If a document has been sent by a third party, that contains information about an individual, which relates to their personal or professional life, it is personal data. An outline of an organisation's standard procedure, relevant to an individual's complaint/section 29 case will not be personal data.