Procedure: Personal Data Request Response

Department: IT

Date: **Approved October 2016** **Review Date:** **September 2018**

1.0 **Purpose**

These procedures set out how to respond to requests for personal information from and about applicants, current and former clients, staff and others whose personal data the company holds in accordance with their rights as data subjects under the Data Protection Act 1998 and the data protection laws of other relevant jurisdictions.

These procedures support the Data Protection Policy and also other policies relating to the management of client and staff records. These procedures form part of 110% Ltd.'s Information Security Policy Framework.

2.0 Scope

The scope of these procedures applies to information that we hold about all current and former 110% Ltd clients or staff, regardless of where or how they were supported or worked.

3.0 Requests by current and former clients and staff for their own personal data

Everyone has the right to know what personal information organisations hold about them, why and how their information is held and used, with whom their information is shared and for what purpose and for how long their personal information is retained. People also have the right to check that the information held about them is accurate and to object to processing of information that would cause them damage and distress.

In the 110% Ltd. context individuals may make requests for their own personal data which can be readily met in the normal line of business e.g. by asking for and receiving feedback on their progress or performance.

The following procedures cover the most common scenarios for managing formal requests by individuals for their own personal data.

Handling Data Subject Access Requests

3.1 Under the UK Data Protection Act, a formal request for one's own personal data is called a data subject access request. However, people do not have to state that they are making a data subject access request, or cite the Data Protection Act, for their requests to be valid. A request by an individual for their own personal data may be simple or complex. The management of all such requests must be governed by a common set of rules.

3.2 All requests must be made in writing

We may not require anyone to complete a subject access request form but we can encourage people to use the form as it provides helpful prompts to focus the request and help staff identify where the relevant information is likely to be held. If someone asks for assistance in completing a request form, it can be helpful if the member of staff completes the form and asks the applicant to affirm that the details are correct and to sign it.

3.3 **Proof of identification**

If the person making the request for their own information (the data subject) is not known to the person receiving it, the data subject must provide proof of their identity in the form of their client ID card, a birth certificate, passport or driving licence.

3.4 **Requests made on behalf of the data subject by a third party**

If someone makes a request on behalf of another person e.g. a lawyer on behalf of a client, the person making the request must provide evidence of their authority to make the request on behalf of the data subject, for instance confirmation of power of attorney, or the written consent of the data subject. If the officer receiving the request is in any doubt e.g. if the signature does not match those on record, it is necessary to contact the data subject to get confirmation of their consent to disclose their personal data to the third party. If the request is for information of a sensitive nature, it may be appropriate to send it to the data subject rather than the person making the request on their behalf.

3.5 **Fees for handling requests**

110% has the right to charge a fee of £10 for processing a subject access request. The level of the fee is fixed by statute. In the case of requests made by current or former clients, the Company Chairman or Company Secretary or their nominees have authority to levy or waive the fee as appropriate under the circumstances. Where requests are made by current or former staff, the Director of Human Resources or his nominees have authority to levy or waive the fee.

3.6 **Statutory timescales for complying with requests**

The statutory deadline for responding to subject access requests is 40 calendar days from receipt of the request (and the fee if levied) or from confirmation of the identity of the person making the request. If the request is very vaguely worded, it is legitimate to stop the clock at the point that the original request is received in order to seek clarification of the information requested.

3.7 **Informing applicants of their rights**

The person managing the request should use and adapt the 110% ltd data protection request acknowledgement and response templates which are provided by Human Resources. These provide information for applicants about their legal rights and support staff in responding consistently and appropriately to requests.

3.8 **Managing straightforward requests**

If a request for personal data is straightforward and not contentious, it should be managed locally by the relevant Department or Service, with advice from Human Resources staff as needed.

Requests from current or former clients: Client Support.

Requests from current or former staff: Human Resources Partner

3.9 **Managing more complex requests**

It is essential to involve colleagues in Human Resources in managing any request which has one or more of the following characteristics:

- Complex or voluminous requiring retrieval and appraisal of information from various sources e.g. " all correspondence, emails, reports relating to my studies…"
- made in the context of an appeal or dispute
- includes information relating to other people (who will have their own rights as data subjects) within or out-with 110% Ltd.
- combines a subject access (information about me) request with an FOI request (How 110% decided….).

Under these circumstances, the Data Protection Officer will discuss the request with the Department or service that has received the request and agree whether the request should be managed by HR or by the Department or Service.

In either case the Data Protection Officer or Information Governance Coordinator will review the information requested and recommend what information should be disclosed or withheld compliance with the relevant provisions of the Data Protection and Freedom of Information Acts.

4.0 Request for Personal Data by Third Parties

4.1 Under most circumstances we must obtain the written consent of individuals before disclosing their personal data to third parties

4.2 **Third party requests to make contact with individuals**

In this context the personal data of current or former clients includes the fact that they are or were a 110% Ltd client. If someone contacts 110% Ltd asking to make contact with a current or former client or expressing concern about their welfare we must not confirm that the person is or was a client. We can offer to take the contact details of the enquirer and to forward these on to the individual concerned if our records confirm that they are or were at 110% Ltd, in order that the individual can chose whether to respond.

4.3 **Disclosure of information about staff: references**

When receiving requests for references about a current or former member of staff it is legitimate for managers to disclose limited personal data necessary to verify the details of their employment and role at 110% Ltd to a potential employer, as long as it is possible to verify that the person making the request

- is who they claim to be,
- has the authority to make the request and
- has the consent of the applicant.

If in any doubt, seek the consent of the data subject.

Staff need to be aware that data subjects have the right to ask the organisation that receives the reference for a copy of it. Both organisations and data subjects have the right to take legal action against the authors of references where they consider that the reference has misrepresented the candidate's abilities.

4.4 **When someone claims legal authority to request personal data**

In some cases, requests for personal data may be received from people claiming legal authority to ask for the information concerned. In these cases, recipients of requests should seek advice from the Data Protection Officer and Information Governance coordinator within Human Resources.

Unless the person making the has a warrant or court order requiring 110% Ltd to disclose personal information about current or former clients, 110% Ltd is not obliged to comply with such requests. Therefore, all staff who receive requests for personal data from the police or other government bodies must follow these procedures to ensure that disclosures of personal data are lawful, authorised, and accountable. Requests from the Police should be managed in accordance with the Procedures for responding to Police enquires and attendance on site.

All requests for disclosure must be in writing, by email or letter. Organisations such as Police Scotland have a standard personal data request form.

The request must

- be signed by an officer with the authority to make the request; this may be an electronic signature or a scanned image of a signed form, if the request is made by email.
- set out the legal authority for making the request. This is normally a specific section of the Data Protection Act. The request must explain how this right applies and why they need the information.

Even if the applicant is known to the person handling the request it is necessary to verify the applicant's identity and their authority to make the request.

4.5 **Authorising disclosure to third parties**

Requests to disclose personal data must be escalated to an officer who has designated authority to decide whether to release or withhold the information.

For requests by the police, Home Office or other government bodies:

- for a client's personal data, the responsible officer is a Company Director or Company Secretary and their nominees.
- for a member or former-member of staff's personal data, the responsible officer is the Director of Human Resources or their nominees.

The responsible officer will need to consider whether

- the disclosure is necessary for the purpose claimed e.g. the prevention or detection of crime or the apprehension or prosecution of offenders;
- not disclosing the personal data would be likely to prejudice the purpose cited.

The responsible officer must be satisfied that the request is reasonable and proportionate and disclose only the minimum personal data necessary for the purpose, seeking advice from the Data Protection Officer as appropriate.

5.0 Security of Communications

All personal data disclosed in response to a request must be communicated by a method appropriate to the security and sensitivity of the information.

Before supplying information it is essential to check how the applicant wishes to receive the information and ensure that you have the correct postal or email address.

Information containing sensitive personal data sent by email or using a USB memory stick or other portable media must be encrypted.

If sending a hardcopy, then the packaging should be marked as strictly private and confidential and sent via recorded delivery.

6.0 Keeping and Audit Trail of Requests

All subject access requests and requests from third parties must be recorded on University systems so that 110% Ltd has an audit trail of actions taken in response to a request and can justify each decision. The record must include details of the request, contact details of the applicant, evidence sought and obtained to verify their identity, the decision to release or withhold the information requested, the reasons for the decision and a copy of any information disclosed.

For requests by and about clients:

Straightforward subject access and third-party requests must be recorded either in the request handling system maintained by the Client Service.

Records of requests from the police or government agencies are held by the Request Registry and reviewed by the Secretary of 110% Ltd.

For requests by and about staff:

Straightforward subject access and third party requests about current staff must be recorded in the individual's personal file held by Human Resources.

Where requests for information are received about former staff, the manager handling the request should liaise with Human Resources and provide a record of the request and the response to Human Resources to add to the leaver's file.

Records of complex requests managed by Human Resources are held in the central data protection and FOI management records managed by HR.

The recommended retention period for request records is completion plus 6 years in line with that for records that need to be retained for a limited time to defend 110% Ltd's legal interests. (The Limitations laws of the UK).

7.0 Monitoring and auditing

This procedure and its implementation will be subject to internal monitoring and auditing, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. 110% Ltd will also undertake appropriate benchmarking and external auditing exercises as may be applicable periodically.

8.0 Associated documents

Please refer to:

- Data Protection Act 1998
- Freedom of Information Policy
- Data Protection Policy

9.0 Review of procedure

This policy will be reviewed at least every two years or when there are significant changes to it.

10.0 Contact list for queries related to this procedure

Freedom of Information Officer

Data Protection Officer

Chief Information Officer

11.0 Authority for this procedure

Senior Management Team