FIN003 CHALLENGERS DATA POLICY

		Date	Amended by:
Date of Issue	1	May 2018	Amanda Matthews
Issue	2		
Issue	3		
Issue	4		
Issue	5		
Issue	6		
Issue	7		
Issue	8		
Date of Last Review			November 2019

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

Contents

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

1. INTRODUCTION

The Data Protection Act 1998

The Data Protection Act 1998 allows individuals certain rights regarding information about them held by Disability Challengers in 'relevant' electronic or manual records. This policy applies to all staff, employees, casual workers, volunteers and trustees. It is to be read alongside and is covered by the 'spirit' of The Disability Challengers (CHALLENGERS) Approach, Employee Handbook and Terms & Conditions of Employment (T&C's). The policy aims to meet the standards and requirements of current legislation and practice for the multi-agency data and information sharing policies of local authorities to whom we provide services as outlined in Appendix 3

General Data Protection Regulation (GDPR)

Challengers also applies the principles of GDPR to the protection of personal data that it holds.

- Data is processed lawfully, fairly and in a transparent manner.
- Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected.
- Data accurate and, where necessary, kept up to date.
- Data is kept in a form which permits identification of data subjects for no longer than is necessary.
- Data is processed in a manner that ensures appropriate security of the personal data.

1.2 Definitions

'Disability Challengers' - CHALLENGERS

'Data Subject' - an individual who is the subject of personal data.

'Personal Data' - information about a living individual (the 'Data Subject') who can be identified from that information.

'Data' - information recorded in manual or computerised form. This can include data held partly on computer files and partly on manual files providing that, when these are taken together, the subject of the data can be identified. It can mean data on computers, mobile phones and photo copiers.

'Relevant Filing System' – any set of information structured by reference to individuals, or by reference to criteria relating to individuals, in such a way that particular information relating to a particular individual is readily accessible.

'Sensitive Data' – amongst other items this can include data regarding subject's racial or ethnic origins, political opinions, religious or other beliefs, trade union membership, physical or mental health, sexual life and the commission or alleged commission of any criminal offences.

'Data Controller' – The Act requires the organisation/charity to be appointed as the 'controller' and a person appointed as the nominated Data Protection lead. Disability Challengers' is the nominated controller, and the Chief Executive Officer (CEO) is the nominated Data Protection lead. The Chief Executive Officer (CEO) has overall responsibility for a compliance with the Data Protection Act (DPA). The CEO should ensure creation, implementation and annual review of a Data Protection Policy (DPP) and related policies, processes and procedures. Day to day monitoring of the compliance could be delegated to senior managers, trustees, staff and members, but responsibility for information risk remains with the CEO.

2. POLICY

2.1 Confidentiality

Personal data is confidential and will be disclosed only for registered purposes to charity staff and other agents of CHALLENGERS when carrying out their work, to others as detailed in the appropriate registration, and to a court under the direction of a court order. Staff whilst aiming to provide appropriate support to children, young

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

people and families, will not offer absolute confidentiality as there may be circumstance as outlined in 5.3 below, when it is impossible to do this.

2.2 Design of Computerised and Manual Record Systems

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself. Computer and manual record systems and files will be designed to comply with the Data Protection principles, which are as follows:

The information to be contained in personal data shall be obtained, and the personal data shall be processed, fairly and lawfully. Personal data shall be held for specified and lawful purposes only. Personal data shall be accurate and, where necessary, kept up to date. Where there are concerns over the accuracy of data it should not be used. Personal data held for any purpose or purposes shall not be kept for longer than is necessary. Reference should be made to Challengers Fair Processing Notice found on the Challengers website: http://disability-challengers.org/privacy-policy/

2.3 Security of Information

Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data. Appendix 4 is a guidance sheet on how to protect data stored on equipment.

CHALLENGERS's computers must not be used for private work, for domestic or recreational purposes or on behalf of other organisations. Manual data records must only be used for their designated purposes.
Please refer to Safeguarding policy OPS001 relating to photographic data gathered by mobile phone or camera.

2.4 Registration

It shall be the responsibility of the Data Controller to complete the registration of CHALLENGERS and to maintain the register entry with the Office of the Information Commissioner (ICO).

Information regarding new systems or files or new uses of existing files shall be provided to the Data Controller in sufficient time to enable amended registration details to be submitted before the new system is brought into use.

2.5 Unregistered Personal Data

Unregistered or inaccurate personal data will not be held. The Data Controller may examine any data to determine the accuracy of registration and staff must co-operate in this process. If unregistered personal data is detected it shall not be processed further until registered or, if it is held for an inappropriate purpose it should be disposed of.

2.6 Quality and Currency of Personal Data

CHALLENGERS will hold the minimum data necessary to enable it to perform its business. The data will be erased once the need to hold it has passed. This stipulation shall, however, be subject to the specific requirements of the CEO, auditors and other bodies who may require data to be held to facilitate the closing or audit of CHALLENGERS's accounts or the inspection of services.

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

Every effort will be made through induction and interim training for staff, as well as regular reminders, to ensure that data is accurate and up-to-date, and that inaccuracies are corrected without unnecessary delay. To this end employees and all data subjects are required to keep CHALLENGERS informed of any changes in their personal circumstances, e.g. marital status, address, telephone numbers, next of kin etc.and also encourage others to notify CHALLENGERS of changes they become aware of in the personal data of others.

Personal Data shall be processed fairly and lawfully and shall not be processed unless at least one of the following conditions is met;

a. Data subject's consent is given;
b. It is necessary for the performance of a contract or with a view to entering into a contract
c. There is compliance with the data controller's legal obligations (but not imposed by contract)
d. It is in the Data subject's vital interests
e. It is required for the Administration of justice
f. It is in the Data controller's legitimate interests – must not prejudice rights and freedoms of the data subject and must inform the data subject at the time of collection the purpose for processing and the legitimate interest it is relying on to process the data.
g. A safeguarding referral is required. Refer to Challengers safeguarding children & young people policy OP001 section 2.4.

If processing sensitive personal data one of the following conditions also have to be met:

a. explicit consent
b. data controller's legal right/obligation in connection with employment
c. to protect vital interests of a data subject (where consent cannot be given /obtained).
d. Legitimate interests of not for profit organisations.
e. Data subject has already made public
f. Legal proceedings
g. Administration of justice

2.7 Access Rights for Data Subjects

CHALLENGERS will make all reasonable efforts to ensure that data subjects are aware of the data which is kept about them, where it is kept and why it is kept. CHALLENGERS will provide any individual who requests access in a reasonable manner a reply stating whether or not CHALLENGERS holds personal data about that individual and, if so, a written copy in clear language of the current data held.

If the information to be provided to a data subject identifies another person in addition to the data subject, the information will not be disclosed unless and until the other person has given written authorisation for the disclosure to be made.

Applicants must supply sufficient information both to confirm their identities, and to locate the data sought. The response to the application will be met as soon as possible and in any case, within one month of the request. The 1 month period commences when CHALLENGERS receives sufficient information to respond to the data subject's request. Where requests are complex or numerous CHALLENGERS will be able to extend the response period by a further two months.

Personnel files are available for inspection by staff, upon advance written request and in the presence of the Head of Department, or the Chief Executive Officer.

2.8 Disclosure of Personal Data

CHALLENGERS may disclose personal data if it is requested for any of the following purposes:

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

Safeguarding Children and Vulnerable Adults cases
The prevention or detection of crime;
The apprehension or prosecution of offenders;
The assessment or collection of any tax or duty.

However, no employee must take it upon him or herself to disclose personal data in any of the above circumstances, except when instructed to do so by a Court Order which has been validated by the Chief Executive or other member of the Senior Management Committee, or when instructed to do so by a legal representative of CHALLENGERS. The only exception to this is Child Protection when the employee should work alongside the Director of Operations.

2.9 Transmitting Data outside of the Organisation

From time to time there will be a valid business requirement to transmit personal data to third parties outside of the organisation. This could be for audit purposes, or in order to provide data to a mailing company. When doing this staff should ensure that:

Data will be passed or transmitted by a secure route

Any data sent in physical form is sent by recorded delivery, by special delivery or by courier in order that it is possible to obtain a receipt to track delivery.

Always refer to Challengers Safeguarding Children & Young People policy OPS001 section 13 (Sharing Data & Reporting)

Before such data leaves the organisation, the permission of the Data Controller must be received in writing, using the form provided in Appendix 1.

With remote access desktop availability for all staff, the sharing of information internally via email, flash drive and memory stick should not now be necessary but if used infrequently, staff should take extra care. These must not contain sensitive or personal data if to be taken outside of the organisation's buildings or ICT infrastructure.

2.10 Procurement of Data Processing suppliers

Please refer to FIN001 Challengers Financial Procedure Policy section 4, which provides a clear guide to the Procurement and Tender process to be followed at all times. Particular note should be made to the requisite clauses that must be included on all contracts entered into, to ensure compliance with this Data Protection Policy and The Data Protection Act 1998.

3. DATA SUBJECT CONSENT

Challengers respects people's preferences on how they wish to be contacted and what they want to hear about. We only contact people that have actively opted in to hear from us. We collect these preferences via our websites – the main organisation website and our booking website, in person or via email communication – they are then stored securely on the Challengers database. We will respect these choices until the data subject chooses to opt out.

If the data subject donates to Challengers, Challengers will contact them with other opportunities to support or donate – this is in line with the guidelines on legitimate interest. If the data subject requests not to be contacted regarding further opportunities to donate, Challengers will respect these choices.

If a parent/carer registers with Challengers the organisation will be able to send them any information relating to bookings and schemes.

When an individual is fully recruited to work at Challengers the organisation will be able to send them any information relating to them working on scheme to enhance their employment with Challengers.

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

When a family registers to use Challengers services they will have the right to decide who their data is shared with. (OPS015 Challengers Children's Information Sheet)

4. WHAT TO DO IF DATA IS LOST OR RELEASED

Appendix 4 is a guidance sheet on how to protect data stored on equipment.

However, a data security breach can happen for a number of reasons:

Loss or theft of equipment containing data
Inappropriate access and poor controls or human error
Hacking or Phishing or blagging offences

In these cases it is important that the organisation should

Contain the source of the data loss and seek to recover any lost data
Assess the data loss and consider the on-going risk
Notify the Information Commissioner's Office, other regulators and the data subject within 72 hours of a breach. The data subject does not need to be informed if the breach is unlikely to result in a risk to the data subject. High risk is typically measured as the likelihood fraud will be committed with the leaked information or that publication of the data could cause the data subject extreme distress or embarrassment.
Evaluate the loss and consider how it can be prevented from re-occurring.
All data losses whether actual or suspected of either electronic or paper based information should be immediately reported to the CEO. (The nominated Data Protection Lead).

Reference should also be made to DC006 Challengers Business Continuity Plan, section 4.

See appendix 5 for the steps to follow in the event of a breach or if you suspect a breach may have happened.

5. POLICY & DATA TRAINING REVIEW

This policy will be reviewed annually, to take account of changing legislation, organisational needs and trends in best practice. Employees and volunteers will receive training on a regular basis on the importance of Data Protection, and is included in the Safeguarding training for all employees. Changes to this policy will be informed to employees as soon as possible and certainly no later than four weeks after effect. This is of importance as indefinite retention is unsustainable and legislative changes need to be reflected in the policy.

6. DATA COLLECTION, STORAGE AND RETENTION

Please see policy number FIN003A for full details on how Challengers collects, uses, stores and how long it keeps personal data within each department during the course of normal business activities.

7. DATA DESTRUCTION

Information held for longer than is necessary carries additional risk and cost. Records and information should only be retained for legitimate business use. Under the DPA 1998, personal data processed by Challengers should not be retained for longer than is necessary for its lawful purpose.

Data reaching its retention period should be reviewed on a regular basis, preferably each quarter, by the department to whom the data is relevant and then signed off for destruction by a member of the Senior

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

Management Team who will ensure that the destruction request is in line with the retention period required by the relevant class of data listed in FIN003A.

Storage and destruction of records can be undertaken by third parties contracted for those purposes. Records must be securely destroyed with a cross cutter shredder, pulped or burned. There should be no paper documents disposed of that have not been shredded first. Processes must be in place to ensure that all backups and copies are included in the destruction of records.

8. RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

Any data subject has the right to have their personal data erased without undue delay. This right is contingent on the occurrence of one of the following:

The data is no longer necessary
The data subject withdraws consent
The data controller has no overriding grounds for continuing the processing against the objection
Processing was unlawful
Erasure is necessary for compliance with EU or national law
The individual objects to the processing and there is no overriding legitimate interest for continuing the processing
The personal data is processed in relation to the offer of information society services to a child.

Challengers can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

To exercise the right of freedom of expression and information
To comply with a legal obligation or for the performance of a public interest task or exercise of official authority
For public health purposes in the public interest
Archiving purposes in the public interest, scientific research historical research or statistical purposes
The exercise or defense of legal claims

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

9. Appendix 1 - Disability Challengers Data Transfer Request Form

Please complete the details below and forward to the Data Controller (CHALLENGERS CEO) before data transmission takes place. Do not pass or transmit data outside of the organisation before permission to do so is given in writing.

Name

Description of data to be transferred

Data recipient

Reason for data transfer

Other Information
(including how data will be transmitted)

Signed by: Date:

This data transfer is / is not approved

Signed by: Date:
(Data Controller)

Reasons – if approval not given

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

10. Appendix 2 - Legislation and Related Policies

The principle legislation controlling the exchange of information is

- The Data Protection Act (1998).
- The Data Protection Act (2017) *(pending commons approval)*
- General Data Protection Regulation (GDPR)
  CHALLENGERS is registered with The Information Commissioner:
  Registration Number Z9094310
- The Human Rights Act (1998)
- The Common Law Duty of Confidence
- The Freedom of information Act (2000)

CHALLENGERS also takes into account the United Nations Convention on the Rights of the Child http://www.unicef.org/crc/files/Rights_overview.pdf especially in this context:

Article 3 – all organisations concerned with children should work towards what is best for each child
Article 12 – children have the right to say what they think should happen when adults are making decisions that affect them, and to have their opinions taken into account
Article 13- children have the right to get and share information, as long as the information is not damaging to them or others
Article 16 – children have the right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes

In addition, Challengers make every effort to comply with but are not affiliated to the following agencies:

Surrey Multi-Agency Information Sharing Protocol (MAISP) developed by representatives from Surrey's county and district councils, the health service and Surrey Police.

http://www.surreycc.gov.uk/sccwebsite/sccwspages.nsf/LookupWebPagesByTITLE_RTF/Information+sharing+protocol+for+multi+agency+staff?opendocument

Hampshire has developed a Children's Trust information Sharing Policy which applies to children and young people up to the age of 18 years.

http://www3.hants.gov.uk/information_sharing_policy_2009_-_trust_version.pdf

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

11. Appendix 3 Competency

In UK Law, a person's 18th birthday draws the line between adulthood and childhood.

3a Gillick or Fraser Competency

The right of younger children /young people to give informed consent that is proportionate to their competence and age is not always a reliable indicator of competence to make decisions. A judgement from the House of Lords in 1983 laid down criteria for determining whether children / young people under 16 were able to consent to medical examination and treatment. These criteria have been used to develop professional practice to determine if children aged 13 years and above are competent to make decisions. A child or young person who has a learning impairment may be Gillick/Fraser competent. This will include making decisions about whether information can be recorded or shared.

3b Mental Capacity of Young Adults

Mental capacity is the subject of legislation and determined by professional assessment. Disabled young adults who have reached the age of majority may not be deemed competent to give informed consent. This includes making decisions as to whether their personal information can be recorded or shared.

CHALLENGERS staff are not trained to assess competency and will seek advice from qualified professionals if situations arise where a disabled young person or young adult may be required , or wish to withhold consent, to give permission for personal information to be recorded or shared. Nevertheless we will strive to ensure that the views of the young person or young adult are taken into account, as much as possible in the taking or sharing of information.

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

12. Appendix 4 - Practical Guidance

1. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

a. Confidentiality means that only people who are authorised to use data can access it.
b. Integrity means that personal data should be accurate and suitable for the purposes
c. Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

2. Security procedures include:

a. Entry Controls – Any stranger seen in entry controlled areas should be reported. All visitors must sign in through daily maintained sign in registers.
b. Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind, ensuring a clear desk policy for all personal information.
c. Methods of disposal - Paper documents should be shredded. Floppy disks and CD-Roms should be physically destroyed when they are no longer required.
d. Equipment. - Users should ensure that individual monitors do not show confidential information to passers-by and they log off from their PC when left unattended.
e. Access to all areas of Challengers during working hours is controlled by security coded doors, daily maintained visitor register.
f. Out of hours, Challengers sites are secured by lockable doors and windows, intruder alarm systems and smoke detectors.
g. Specific data storage areas are secured by intruder access alarms, smoke alarms and locked doors at all times.

3. Providing information over the telephone:

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

a) Suggest that the caller put their request in writing.
b) Refer to their line manager or the Data Protection Compliance Manager.

Hard Drives

Hard Drives can be packed full of sensitive information. It is CHALLENGERS policy that no sensitive or personal data should be stored on the local hard drive of any CHALLENGERS issued laptop, mobile phone or other device which has a hard drive. Please also see the measures and any equipment listed under the section ‘Bring Your Device To Work’ below.

CHALLENGERS uses an approach to ensure that all copying to a shared printer is done using a PIN. It is imperative that CHALLENGERS deletes all information on the hard drive on a regular basis but essentially, at the end of copier’s life before disposal.

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

Use of Removable Media

The use of removable media devices (RMDs) – for example, memory sticks; external hard drives – will only be approved if there is a valid justification for its use: clear business benefits must be demonstrated and must outweigh the risks before approval will be given. Refer to point 2.9 of this policy.

- Requests for access to, and use of, RMDs should be made to the SMT with an associated justification.
- All employees must only use RMDs to store or share information in accordance with agreed procedure

The Print Server

Most digital photocopiers see the print server is embedded in the machine and it is the print server part of the machine that may hold the most vital information. The Print Server should be cleared of all information on a regular basis but essentially at the end of the copier's life.

Scanner

The machine may hold data on individual workstations and passwords. Machines with the facility to scan to email will hold private email addresses of individuals within the corporation or organisation. All scanner and email information should be removed on a regular basis but essentially at the end of its life.

Print Queue

Often held in the RAM of the machine pending print jobs can contain sensitive information. Often the digital copier is replaced due to unreliability and by simply clearing a paper jam the machine can start printing out a wealth of information. When this occurs it is important to clear all pending print jobs.

Bringing Your Own Device to Work

Reference should be made to OPS001 Challengers Safeguarding Children and Young People section 5 and HR001 Challengers Staff Handbook section 7.7, outlining our policy relating to the use of personal phones and connected devices both in the workplace and when working from home.

If, in line with the above policies, exceptional circumstances necessitate the use of personal phones or devices, the following measures and guideline must be adhered to, to protect personal data:

- Ensure the device is pin/password protected
- Implement automatic screen lock after a short period of inactivity
- Ensure that anti-virus software is implemented and updated on a regular basis.
- Do not save personal data relating to any Challengers personnel or service user on local hard drives
- Do not use USB or RMDs unless specifically provided and requested by Challengers
- Only to access personal data through Challenger's secure remote desktop application or Office 365
- Photographs, videos or images of children should never be captured, transmitted or stored on personal devices in line with FRC005 Challengers Photo Policy
- Do not send any personal data relating to and Challengers personnel or service users outside of the Challengers network, through any personal email account. (Refer: FIN003 section 2.9)

Challengers will not reimburse any employee for the running costs or damage to any unauthorised personal device used in connection with Challengers.

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

The existing Data Protection training will ensure that clear understanding is made with reference to using any personal device in the workplace or when working from home.

If Challengers have good reason to believe these measures and guidelines are being breached, they reserve the right to check any personal devices in the workplace.

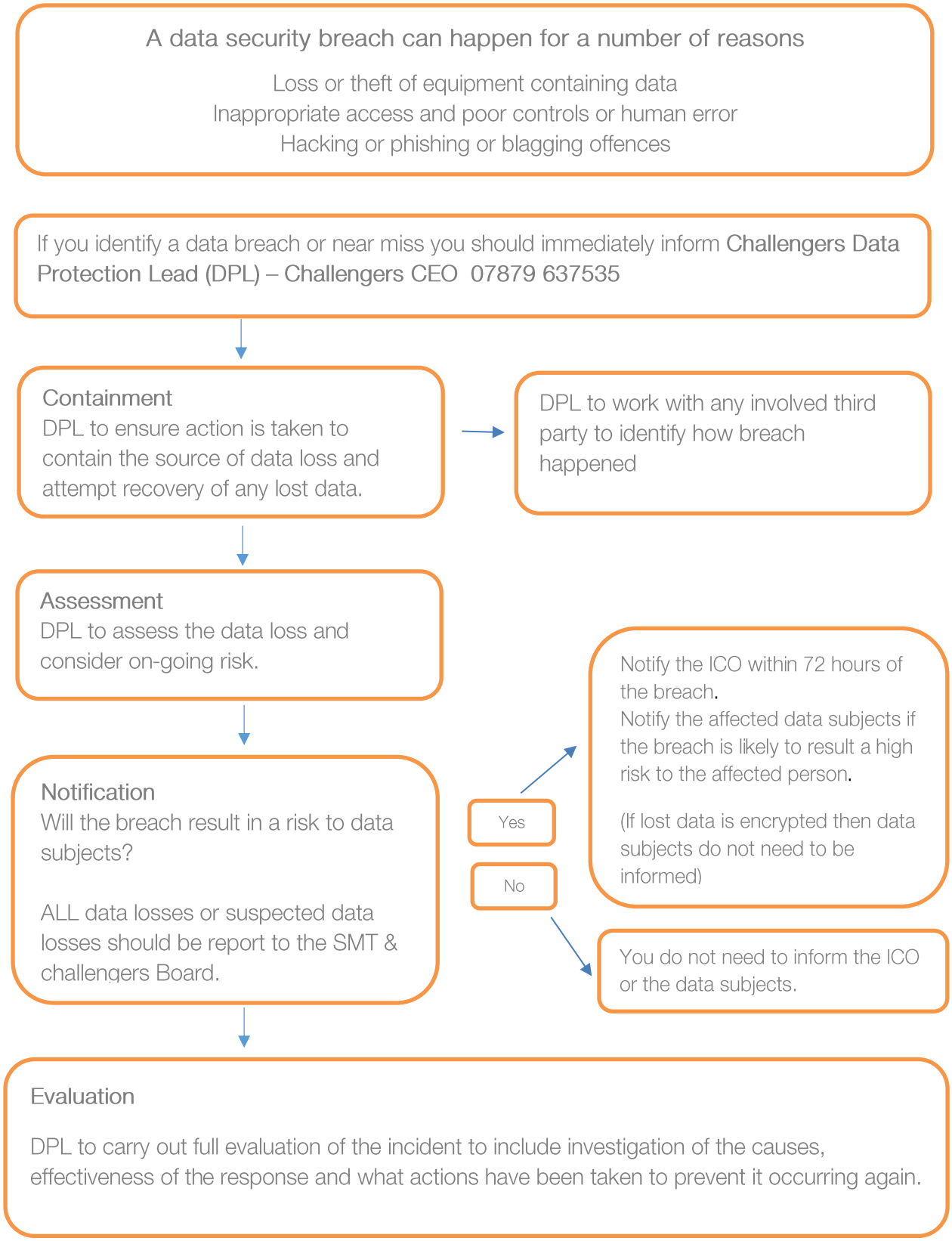
Fair Processing Notice

For full details of how any data collected by us or provided by donors, service users, volunteers or staff members is processed, please refer to:

www.disability-challengers.org/privacy-policy/

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

13. Appendix 5 – What to do if a Data Breach Occurs



14. Appendix 6 – Data Protection Incident Response Evaluation Form

Data Protection Incident Response Evaluation Form

Date of Incident: …… DPL: ……

1. What data is involved?	
2. How has the data been shred/lost/accessed?	
3. How long has the data breach been occurring?	
4. How was the data breach discovered?	
5. How many data subjects are involved?	
6. Has the data been made available to non-intended people?	
7. Where is the data now and is it known how many people accessed it? If yes how many?	
8. How many unauthorised people may have accessed it?	
9. What is being done to recover the data?	
10. Did the breach included sensitive data?	

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

11. Who has been told about the data breach?	
12. What action has been taken to prevent this incident from happening again?	
13. Which policies are in place covering the handling of the data and its security?	
14. What training/awareness raising measures have been taken in light of this incident?	
15. Has this happened before?	

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

Modifications made to this document since its issue are as follows:

15. DOCUMENT CHANGE HISTORY

Summary of Change	Section no / page no	Changes made by	Release date
General review and change to require staff personnel records and CRB checks to be kept for 25 years	Page 7	Laura Sercombe	February 2014
General policy review following data protection audit.	Items 1 & 1.2 page 3 Items 2.2, 2.3, 2.4 & 2.6 page 4 Items 2.6 & 2.8 page 5 Items 2.9,2.10,3 &4 page 6 Item 6 page 9 & 10 Appendix 10 2 (f&g) 3 page 14 Appendix 4 Item 3 page 15 & 16	Amanda Matthews	March 2017
Access rights Challenges response time update in line with GDPR.	2.7 Access rights	Amanda Matthews	August 2017
What to do if a Data Breach Occurs flow chart added Data protection incident response evaluation form added Update to include GPDR breach notification guidance	Appendix 5 Appendix 6 Section 3 Section 2.6	Amanda Matthews	October 2017

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390

Update to include GPDR guidance on legitimate interest Section added on Right to Erasure (Right to be Forgotten) in line with GRPD	Section 7		
GDPR Data subject consent Data collection, use & storage	Introduction Section 3 Section 6	Amanda Matthews	May 2018
General Review		Amanda Matthews	November 2019

S:\ADMINISTRATION\POLICIES AND PROCEDURES\ORIGINALS - DO NOT DISTRIBUTE\FIN003 CHALLENGERS DATA POLICY.DOCM

Challengers, Stoke Park, Guildford, GU1 1TU | www.disability-challengers.org | 01483 579 390