**My organisation needs me to complete a Data Protection Impact Assessment - what information do I need?**

**This document contains possible questions and answers you may need in regard to the Prove It! site, based on previous requests we have received.**

**If you need any additional information, please contact us for support.**

**What is the project about?**

**Why do you need to collect this information? Explain broadly the purpose of the processing and what the project aims to achieve. Clearly describe the intended effect on individuals, the benefits of the processing – for your service and more broadly?**

You may want to include our information about Prove It!:

*What is Prove It!?*

Prove It! is an online tool developed by Better Communication CIC to support services and settings in measuring the impact of their work supporting children and young people with speech, language and communication needs.

This online resource contains a variety of tools designed to help you gather evidence of the impact of activities you deliver using the Balanced System® five Strands and three levels. This includes tools to measure impact seen by parents and carers, experienced through changes to the environments that children and young people are in, supporting the workforce, identifying need in children and young people and the impact of interventions. Voices of different users across the system are captured through the variety of tools.

The tools focus on questions which offer a place to describe and upload evidence of functional change, the impact of provision and how it relates to the Balanced System® Strands and Levels. The intention is that the evidence is gathered from people who know the children and young people well and can observe that functional change, this may be parents, setting staff, or the child or young person themselves.

*Why has Prove It! been created?*

Measuring impact is regularly discussed however difficult to achieve. Services are often asked to collect information about what they do (inputs) rather than the difference they have made (impact). The purpose of Prove it! tools are to support services and settings to easily collect functional impact evidence. Crucially,

gathering impact evidence from parents, carers and families is at the centre of this approach. The ultimate outcome is to develop the knowledge and capacity for outcomes setting and impact measurement for children and young people with speech, language and communication needs.

**What personal information will be collected?**

* Name of parent, email address of parent, child’s name, photograph or video – all may be provided on a voluntary basis i.e. not compulsory within the system.
* Questions asked in Prove it relate to parental views of the support they have received from the SLT service and the impact this support has had on them and their child
* Name and email address of other professional accessing support via the service, for example school staff, health visitors, other specialist staff
* Questions asked in Prove it relate to views of the support they have received from the SLT service and the impact this support has had on them and children they work with

**How will the individuals know that you are processing their information? What information will you give individuals about this new system / process and how will you support their data protection rights? Have you considered the need for a privacy notice to outline and inform this new processing?**

The website has a privacy notice.

The first time a user logs in, they are asked to agree to the user terms which details their data protection rights and how to exercise them.

Details regarding the Better Communication Privacy Policy can be found here: <https://www.bettercommunication.org.uk/privacy/>

**What is the name of the website?** <https://proveit.thebalancedsystem.org/>

**What is the name of the Company providing the website**?

Better Communication CIC <https://www.bettercommunication.org.uk/>

**How do you intend to share the Personal Data / Special Category Data securely? What methods will you use to protect the information in transit?**

No intention to share personal data.

The website runs over https so that all traffic is encrypted between a user’s computer and the web server.

Better Communication will have access to the data in anonymised format

**Will any data be held or processed outside the HSC (NI) network and if so where? How will you safeguard any international transfers?**

Data will be held in a secure data centre in the UK run by Node4. No data will be transferred internationally except for:

• storage on Google Cloud whose servers are based in the US

• data backups using a backup service based in the US

**Where will the data be stored?**

Externally – Cloud provider, Third Party Servers (including other NHS organisations), AWS or Azure

**Where will the New System be hosted?**

Externally – Cloud provider, Third Party Servers (including other NHS organisations), AWS or Azure

**Which Cyber Security accreditations does the Hosting provider hold?**

**X** ISO:27001 - 2013

**X** Cyber Essentials

**X** Other – please specify: **See https://node4.co.uk/awards/**

**Where will the data be geographically stored?**

**X** Within the UK and meets the new GDPR/DPA18 requirements

https://node4.co.uk/our-services/data-centre-hosting/

<https://cloud.google.com/about/locations#europe> **(London europe-west2 location)**

**Which of the following are applicable for the website?**

**X** A Process to scan for common vulnerabilities?

Is this carried out internally or by a registered third party? This is carried out internally

**X** Secured by design or built using other recognised frameworks (For example NIST)

**X** All data in transport is encrypted.

**X** The site/resource/application requires a password

**X** Passwords require a minimum length and complexity requirement, including a lockout policy after too many failed attempts?

**X** The system validates/sanitises input from all untrusted sources?

**X** The website is served over https

**X** Any external connection made by the application or website to transfer data is encrypted

**X** Users have individual logins

**X** Users have Defined Access Privilege, and restriction to resources based on permission level

**Will it provide reports of attempted or successful breaches of its systems, impacts, and actions taken?**

Only if our data was impacted

**If the Service decided to switch providers, end the contract or take our systems and data in-house, what will it take to migrate the systems and data?**

Data migration would not be possible

**If data migration will not be possible your Service must provide a plan for the destruction of the data at the termination of the contract and explain how your Service will function without this data?**

Better Communication has a data destruction policy available on request.

**Does the system collect usage data?**

No

**Backup of data (How will the data stored in the system be backed up?)**

**X** Backups are taken regularly (Based on the data type and criticality of the System)

**X** Backups stored in a secure location **Node4 data centres**

**X** Backups are encrypted and only available to key members of staff? **Yes**

**X** Backups are kept offsite, and within the UK/EU **Iteracy office https://www.iteracy.com**

**X** Backups are kept outside of the UK/EU **Backblaze data centres in US**