**Data Protection Impact Assessment**

\*\*\*\*Team Area ie. Fife\*\*\*\* Augmentative and Alternative Communication Team (\*\*\*\*Speech and Language Therapy Org\*\*\*\* ) Patient Communication Devices

**Information Governance**

**& Security**

DPIA Version 1.0

**\*\*\*\*Team Area ie. Fife\*\*\*\* Augmentative and Alternative Communication Team (\*\*\*\*Speech and Language Therapy Org\*\*\*\* ) Patient Communication Devices**

**Data Protection Impact Assessment**

DOCUMENT CONTROL

KEY INFORMATION

|  |  |
| --- | --- |
| Title | \*\*\*\*Speech and Language Therapy Org\*\*\*\* Patient Communication Devices |
| Date Issue/Pub | <Date> |
| Date Effective From | <Date> |
| Version/ Issue # |  |
| Document Type | Data Protection Impact Assessment (DPIA) |
| Document Status | Draft |
| Classification |  |
| Owner | \*\*\*\*Speech and Language Therapist\*\*\*\*\* |
| Approvers | ISM, DPO and Caldicott Guardian |
| Contact | Josh Stokes, Digital Health and Care Information Governance, Scottish Government. ([dhcig@gov.scot](mailto:dhcig@gov.scot)) \*\*\*Change to local contact\*\*\* |
| File Name | N/A |

CHANGE RECORD

|  |  |  |
| --- | --- | --- |
| Version | Date | Summary of Changes |
| V1.0 | 18/04/2023 | Initial Draft |
|  |  |  |

APPROVALS

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Name | Designation |
| V1.0 | 18/04/2023 | Josh Stokes | Information Governance Manager, Digital Health and Care, Scottish Government |
|  |  |  |  |
|  |  |  |  |

DPIA DECISION

**Your DPIA has been reviewed and Rejected/Approved by NHSS \*\*\*\*Team Area ie. Fife\*\*\*\* Information Governance and Security.**

**RENEWAL DATE**

Your next review date is [?] months from the date of this DPIA approval.

It should also be noted that your manual and digital processes may require a further data protection assessment or amendment, at any point, before the renewal period as the process develops.

REVIEWING IG & SEC OFFICER NOTES

1.

CONTENTS TABLE

This is a Data Protection Impact Assessment (DPIA) produced by \*\*\*\*NHS Scotland Health Board\*\*\*\* Information Governance and Security for the implementation and management of the XXXXXXX solution.

The assessment documentation consists of this document and a compressed directory containing applicant evidential and reference documentation.

|  |  |
| --- | --- |
| **Section** | **Title** |
| **1.0** | **Introduction and Questionnaire** |
| **2.0** | **Assessment** |
| **3.0** | **AL/ML/Automated Processing** |
| **4.0** | **Technical Summary** |
| **5.0** | **Technical Diagrams** |
| **6.0** | **Organisational and Technical Controls** |
| **7.0** | **Documentation Table** |
| **8.0** | **Principles Assessment** |
| **9.0** | **Risk Assessment** |
| **10.0** | **Acceptance** |
| **11.0** | **Appendices** |

For further information about this DPIA, please contact: \*\*\*\*NHS Scotland Health Board\*\*\*\* Information Governance and Security.

I.0 INTRODUCTION AND QUESTIONNAIRE

(DO NOT DELETE)

**About the Data Protection Impact Assessment (DPIA)**

The DPIA is an assessment tool which is used to identify, assess and mitigate any actual or potential risks to privacy created by a proposed or existing process or project that involves the use of personal data. It helps us to identify the most effective way to comply with our data protection obligations and meet individuals’ expectations of privacy.

An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Failing to manage privacy risks appropriately can lead to enforcement action from the Information Commissioner’s Office (ICO), which can include substantial fines. The DPIA is just one specific aspect of risk management, and therefore feeds into the overall risk management processes and controls in our organisation.

A DPIA is not a ‘tick-box’ exercise. Consultation may take a number of weeks to complete, so make sure that key stakeholders are engaged early, and that your project plan allows for this so that you have enough time prior to delivery to iron out any issues.

Carrying out a DPIA is an iterative process. Once complete, a review date within the next 3 years must be set. Should a specific change in purpose, substantial change in service or change in the law occur before the review date, the DPIA must be re-done.

The [ICO code of practice on conducting privacy impact assessments](https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf) is a useful source of advice.

**Is a DPIA required?**

If the process or project that you are planning has one or more the aspects listed in the questionnaire below then you must complete a DPIA at an early stage.

|  |  | **YES/NO** |
| --- | --- | --- |
| 1. | The work involves carrying out a ***systematic and extensive evaluation*** of people’s personal details, using ***automated processing (including profiling).*** Decisions that have a ***significant effect*** on people will be made as a result of the processing.  Includes:  Profiling and predicting, especially when using aspects about people’s work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements  Processing with effects on people such as exclusion or discrimination  Excludes:  Processing with little or no effect on people | **YES/NO** |
| 2. | The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to criminal convictions and offences.***  Includes:   * Racial or ethnic origin data * Political opinions data * Religious or philosophical beliefs data * Trade Union membership data * Genetic data * Biometric data for the purpose of uniquely identifying a person * Health data * Sex life or sexual orientation data * Data which may generally be regarded as increasing risks to people’s rights and freedoms e.g. location data, financial data * Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive   To decide whether processing is ***large scale*** you must consider:   * The number of people affected by the processing, either as a specific number or as a proportion of the relevant population * The volume of data and/or the range of different data items being processed * The duration or permanence of the processing * The geographical extent of the processing activity | **YES** |
| 3. | The work involves carrying out ***large scale*** and ***systematic monitoring*** of a ***publicly accessible area.*** Includes processing used to observe, monitor or control people. | **NO** |
| 4. | The work involves ***matching or combining datasets*** e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset. | **NO** |
| 5. | The work involves processing personal data about ***vulnerable groups.***  This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data. | **YES** |
| 6. | The work involves ***significant innovation*** or use of a ***new technology.*** Examples could include combining use of finger print and face recognition for improved physical access control; new “Internet of Things” applications. | **No** |
| 7. | The work involves transferring or accessing personal data across borders ***outside the UK.*** | **NO** |
| 8. | The work involves processing that will ***prevent people from exercising a right*** or using a service or a contract e.g. processing in a public area that people passing by cannot avoid. | **NO** |

**Preparing Your DPIA:**

1. **Consultation Phase**

Consult with all stakeholders about what you wish to do as early as possible in the process. Stakeholders will normally include:

* Key service staff e.g. those who will be managing the process.
* Technical support, especially if a new system is involved. This may involve the relevant IT supplier.
* Information governance advisors e.g. Caldicott Guardian, Information Security Officer, Data Protection Officer.

Sometimes it will be necessary to consult with service users. This will be particularly relevant if the change in process will change how they interact with our NHS Board, or what information is collected and shared about them.

Early consultation will ensure that appropriate governance and security controls are built into the process as it is being designed and delivered, rather than being ‘bolted on’ shortly before the change is launched.

1. **DPIA Drafting**

The responsibility for drafting a DPIA will normally sit with the service area that ‘owns’ the change, however, all stakeholders will have an input. Depending on the nature and complexity of your proposal, more than one service area and/ or Information Asset Owner (IAO) may be the owner(s).

1. **Approval and Sign-off**

When a DPIA has been fully completed, it must be submitted for formal review by an appropriate IG professional/ the Data Protection Officer. They will review the DPIA to ensure that all information risks are fully recognised and advise whether appropriate controls are in place. The Data Protection Officer (DPO) will decide, where the DPIA shows a high degree of residual risk associated with the proposal, whether it is necessary to notify the ICO. It may be necessary to inform and/or involve the Board’s Senior Information Risk Owner (SIRO) as part of this risk assessment and decision-making. Once reviewed and if approved, the DPIA will be signed-off by the Information Asset Owner(s) (IAO), normally a head of service. You will receive a PDF version of the approved DPIA. Please keep it safe.

2.0 ASSESSMENT

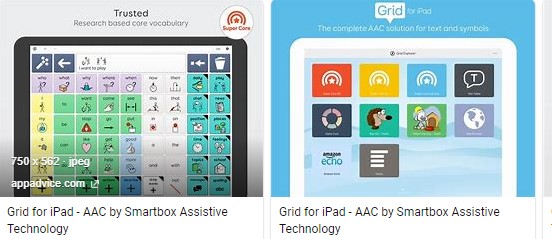
2.1 Introduction

\*\*\*\*Team Area ie. Fife\*\*\*\* Augmentative and Alternative Communication Team (\*\*\*\*Speech and Language Therapy Org\*\*\*\* ) is a regional Augmentative and Alternative Communication (AAC) team. The team is funded by \*\*\*\*Local Health Board\*\*\*\* Health Board and operated in conjunction with \*\*\*\*Local Authority\*\*\*\* who undertake assessments, provide recommendations and provision and provide ongoing maintenance of communication equipment (hardware and software) for clients (children and adults) with complex communication difficulties. These individuals rely on \*\*\*\*Speech and Language Therapy Org\*\*\*\* and the devices provided to communicate, either as their mains means or as a backup system.

The \*\*\*\*Speech and Language Therapy Org\*\*\*\* service was created to comply with the AAC requirement within an amendment to the Health (Tobacco, Nicotine etc. and Care) (Scotland) Act 2016 (part 4), which can be viewed [here](http://www.legislation.gov.uk/asp/2016/14/part/4/enacted). [Further guidance was published in May 2018](https://www.gov.scot/publications/guidance-provision-communication-equipment-support-using-equipment/) to accompany the legislation, containing an AAC vision, principles of communication and support, practical information and references.

The commencement of the law took effect in March 2018- **46A Provision of Communication equipment.** It states that the Scottish Ministers must, to such extent as they consider necessary to meet all reasonable requirements, provide or secure the provision of “*communication equipment, and support in using that equipment to any person who has lost their voice or has difficulty speaking*”

2.2 AAC Devices and Solutions





Within \*\*\*\*Team Area ie. Fife\*\*\*\*, \*\*\*\*Speech and Language Therapy Org\*\*\*\* is responsible for providing the communication equipment (the equipment) to the client. \*\*\*\*Speech and Language Therapy Org\*\*\*\* do not go through the \*\*\*\*Local Authority\*\*\*\* process of requesting equipment, they identify what is required and go straight to procurement to purchase the software and hardware for this function. Hardware and software supplied as a package from the supplier, it is then given a local \*\*\*\*Speech and Language Therapy Org\*\*\*\* number and added to the \*\*\*\*Speech and Language Therapy Org\*\*\*\* asset list, this is then provided to clients on a loan basis for as long as is required. Client needs can be changing, sometimes at a rapid pace, so it is not financially feasible to gift the products as this would result in a large number of unused products and wastage.

By carrying out this process there is no accountability for the devices and software as they bypass the asset tagging process and there is no registration of devices therefore the disposal of hardware becomes more of a risk as it is important at this stage for the devices to be disposed of properly. A process is be developed for this by \*\*\*\*Local Authority\*\*\*\* and \*\*\*\*Speech and Language Therapy Org\*\*\*\* meaning the equipment is returned to \*\*\*\*Local Authority\*\*\*\* and disposed of correctly and securely. \*\*\*\*Local Authority\*\*\*\* is also looking at a Managed Service to ensure appropriate security when lost or stolen.

Devices to enable \*\*\*\*Speech and Language Therapy Org\*\*\*\* such as Hardware laptops and desktops and the appropriate software are purchased through the \*\*\*\*Local Authority\*\*\*\* procurement process and imaged and secured. The \*\*\*\*Speech and Language Therapy Org\*\*\*\* have dual accounts, as well as an \*\*\*\*NHS Scotland Health Board\*\*\*\* account they also have a \*\*\*\*Local Authority\*\*\*\* account which allows access to their network and are given the necessary access to carry out their function with the organisation.

AAC equipment requires personalisation to be effective for the client. This means that each device, as well as having generic messages, will also have bespoke personalised vocabulary. This vocabulary normally contains information relating to the client’s life, such as information about their family, friends, medical condition and needs and contact details e.g. e-mail address. The information can be in verbal and picture format depending on the client’s communication needs.

A range of devices and software are used, including Windows and IOS systems. The number of devices allocated to clients at present is 125. The software on many of the devices is backed up by the team or by staff supporting the client to ensure bespoke vocabulary can be quickly re-established should the device require to be reset.

Depending on the client’s needs they may require assistance to use their AAC device. It will be for the client and/or their carer’s to decide on access controls with input from \*\*\*\*Speech and Language Therapy Org\*\*\*\* staff.

2.4 Key Contacts

|  |  |  |  |
| --- | --- | --- | --- |
| Role | **Name** | **Position** | **Email Address** |
| NHS Head of Service (Local area) |  |  |  |
| \*\*\*\*NHS Scotland Health Board\*\*\*\* Clinical Lead |  | Specialist Speech and Language Therapist |  |
| \*\*\*\*Local Authority\*\*\*\* Lead |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

2.5 Controller and Processor

|  |  |
| --- | --- |
| The CONTROLLER is: | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| The PROCESSOR is: | **\*\*\*\*Local Authority\*\*\*\***; - Storage of data within \*\*\*\*Local Authority\*\*\*\* Server will be moved to SharePoint IDC.  **Smartbox**: Hardware/Software Provider, Cloud Storage for Accounts  Smartbox Assitive Technology  Ysobel House, Enigma Commercial Centre  Sandys Road  Malvern, WR141JJ  Email Info@thinksmartbox.com  Phone: 01684578868  **Tobii Dynavox** - Hardware/Software Provider, Cloud Storage for Accounts  Sheffield Technology Parks  Cooper Building  Arundel Street  Sheffield  S1 2NS  Phone: +44 (0) 114 481 00 11  E-Mail: [sales.uk@tobiidynavox.com](mailto:sales.uk@tobiidynavox.com)  **Liberator** -Hardware/Software Provider, Cloud Storage for Accounts  Whitegates, High Street Swinstead, Lincolnshire, United Kingdom, NG33 4PA  Email: Info@liberator.co.uk |

2.6 Sub-Processors and Sub-Contractors

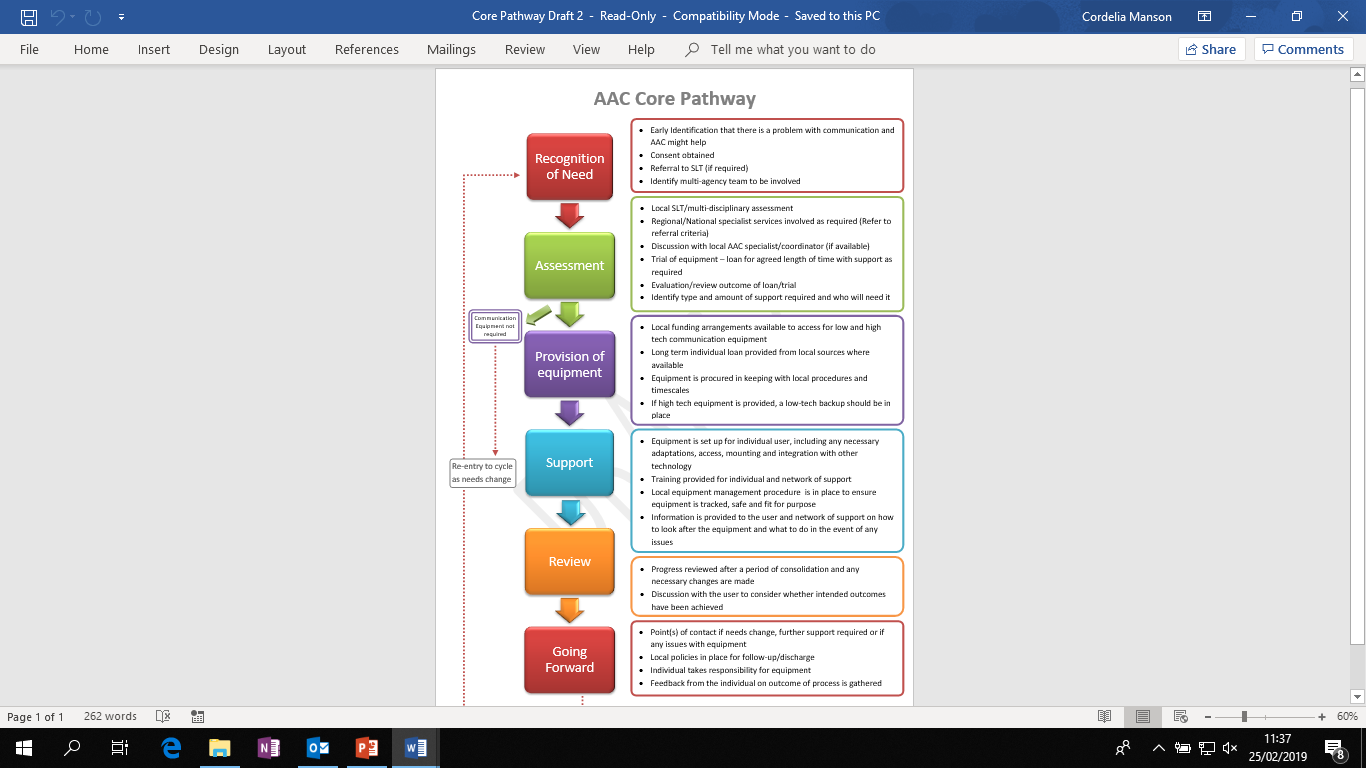
|  |  |  |
| --- | --- | --- |
| Company | **Address** | **Purpose of Sub-Processing** |
| AWS | 1 Principal Place  Worship Street  London | Customer database storage and hosts KeyedIn Infrastructure |
| Dropbox | San Francisco, California | Backups for \*\*\*\*Speech and Language Therapy Org\*\*\*\* Clients data and updating of services. See attached Risk Assessment in documents table. |
|  |  |  |

2.7 Websites

|  |  |
| --- | --- |
| Name | **Website address** |
| Tobii Dynavox | [Tobii Dynavox Global: Assistive technology for communication](https://www.tobiidynavox.com/) |
| Smartbox | [Smartbox - Assistive technology for everyone (thinksmartbox.com)](https://thinksmartbox.com/) |
| Liberator | [Liberator - Homepage | Liberator Ltd](https://www.liberator.co.uk/) |
| \*\*\*\*Local Authority\*\*\*\* |  |

2.8 Data Processing Overview

National AAC Pathway 2018



**\*\*\*\*Speech and Language Therapy Org\*\*\*\* Stages of Intervention**

**This is an EXAMPLE. Please add your own local area Intervention Stages**



Responsibility for ongoing programming and back up of device with **core team**

*\*\*\*Local Team\*\*\** will still be able to access client backups from cloud systems if required, as passwords from initial set up will still be valid

Data programmed by **core team** seeking consultation and support as required.

Data programmed by **\*\*\*Local Team\*\*\*** but **core team** beginning to take a role at this stage with support. SLT service may not be involved at this point.

Data programmed by **\*\*\*Local Team\*\*\*. SLT** for client may also be involved at this stage.

**Controller** of data moves as intervention progresses through the 4 stages

**\*\*\*\*Speech and Language Therapy Org\*\*\*\* - Overview of referral and use of client data**

* Referral to \*\*\*\*Speech and Language Therapy Org\*\*\*\* - Referrals come from NHS (80%)/Education/Social work/Client (20%)
* Assessment and Recommendation of Device/software made by \*\*\*\*Speech and Language Therapy Org\*\*\*\* team – equipment from loan bank for as long as client requires.
* \*\*\*\*Speech and Language Therapy Org\*\*\*\* team – Speech and Language Therapists (SLT) (Health), Teacher and Technician(Education) – liaise with referrer/core team/client to develop software to match client need – at this point collection of personalised info of clients
  + names/
  + places
  + activities
  + personal care info
  + photos etc…

Will be collected and used, to personalise the generic information on the device, to meet clients bespoke communication needs. At this stage, most of the information will be added by the \*\*\*\*Speech and Language Therapy Org\*\*\*\* team.

* IOS equipment – \*\*\*\*Speech and Language Therapy Org\*\*\*\* generate and install ITunes accounts to be used to download recommended software.
* We also use dedicated communication devices/software on windows systems – bespoke backup software from each company supplying devices,
  + Tobbi Dynavox
  + Smartbox,
  + Liberator

is used to back up client prepared information – each client has their own bespoke account/password. Storage used for all systems are cloud based.

* Programming may be done on the recommended device or \*\*\*\*Speech and Language Therapy Org\*\*\*\* team computers and then transferred to client device. \*\*\*\*Speech and Language Therapy Org\*\*\*\* computers are council owned. The PC’s used by the \*\*\*\*Speech and Language Therapy Org\*\*\*\* are not connected to the NHS network.
* Client database and referral information is currently stored on an on premise server with \*\*\*\*Local Authority\*\*\*\*; this server is supported and backed up on a daily basis. As \*\*\*\*Local Authority\*\*\*\* moved to SharePoint a considerable time ago there was dispensation given to allow the continuation of the on premise server to be used by \*\*\*\*Speech and Language Therapy Org\*\*\*\* . \*\*\*\*Local Authority\*\*\*\* are now moving forward and having all the data transferred to SharePoint and are engaging with \*\*\*\*Speech and Language Therapy Org\*\*\*\* to migrate the relevant data to the SharePoint platform. As \*\*\*\*Local Authority\*\*\*\* have been using SharePoint now for 2 years all the necessary security has been imbedded over the time and will be a safe and secure option for the data. The migration of the data when it is programmed will be done in line with proper processes and change management guidance. The existing server will then be decommissioned using the correct \*\*\*\*Local Authority\*\*\*\* processes. There is no input from \*\*\*\*Local Authority\*\*\*\* for confirmation on platform, location, security or processes). Server is accessed by \*\*\*\*Speech and Language Therapy Org\*\*\*\* members given access and \*\*\*\*Local Authority\*\*\*\* business support and IT maintenance when required.

**Adult Learning Disability**

Key staff may be family/social work staff or from 3rd sector organisation, such as Leonard Cheshire, Scottish Autism and Richmond Fellowship.

Restrictions pass codes are activated on IOS devices, to restrict client access to inappropriate content – in discussion with core team.

* Restrictions pass codes are also placed on the communication software to prevent accidental deletion of software /editing – password only shared with key staff members (Family, Social Work and engaged 3rd Party Sector Organisations).
* Key staff members/family are trained in the programming of the software to allow amendments /additions to the communication programme to be made, to ensure it is kept up to date and functional for the client. At this point, programme control moves towards the core team which consist of Care staff, Family, Teachers, Social Work day care staff and Respite staff who support the client , rather than \*\*\*\*Speech and Language Therapy Org\*\*\*\* , once capacity of core team is built.
* Back up information (set up for each individual client – cloud based storage) is shared with key programmers (key staff) to ensure changes are captured at regular intervals, in case of issues with programme, where re-installation may be required.
* This information is held in back up storage for as long as client is on \*\*\*\*Speech and Language Therapy Org\*\*\*\* caseload. At point of discharge, information on device/back up/\*\*\*\*Speech and Language Therapy Org\*\*\*\* computer is deleted.

**Adult Acquired – Key staff -SLT/family/Care home staff**

* Following referral, \*\*\*\*Speech and Language Therapy Org\*\*\*\* will prepare devices and programme software/adding in bespoke personalised vocabulary as requested by client. Restrictions are not placed on devices for adults with acquired conditions unless deemed appropriate.
* Software used by adults with acquired issues often will incorporate access to email accounts / texting/internet/ you tube/social media platforms via the grid communication software to maintain all aspects of communication. This is increasingly requested as adults are using these features routinely and wish to maintain function and independence.
* Each client will have an individual Smartbox/grid account( cloud based) to allow back up of their bespoke information – this is based around Dropbox
* Clients may supply access to their banked voice login details (a 3rd Party organisation, such as Speak Unique creates the clients voice through a series of statements over a period of time which is unique to the client) to \*\*\*\*Speech and Language Therapy Org\*\*\*\* , to allow their personalised voice to be added to grid programme.
* With client permission/consent, they give authorisation for remote editing by the \*\*\*\*Speech and Language Therapy Org\*\*\*\* Team– this allows \*\*\*\*Speech and Language Therapy Org\*\*\*\* team to make changes on \*\*\*\*Speech and Language Therapy Org\*\*\*\* computer to client grid layout and avoid clients communicate systems being removed This is carried out via the Smartbox or Tobbi Dynavox cloud and backed up to the \*\*\*\*Local Authority\*\*\*\* \*\*\*\*Speech and Language Therapy Org\*\*\*\* Cloud Server. As before, family /key staff are taught to programme and back up.
* This information is held in back up storage \*\*\*\*Team Area ie. Fife\*\*\*\* \*\*\*\*Speech and Language Therapy Org\*\*\*\* Server which is backed up on a daily basis or Dropbox for as long as client is on \*\*\*\*Speech and Language Therapy Org\*\*\*\* caseload. At point of discharge, information on device/back up/\*\*\*\*Speech and Language Therapy Org\*\*\*\* computer is deleted.

**Paediatric - Key Staff - Family/SLT/Education staff**

* Restrictions pass codes are put onto IOS devices to restrict client access to inappropriate content – in discussion with core team. Restrictions pass codes are also placed on software to prevent accidental deletion on software /editing – password only shared with key staff members when programming
* Initial programming carried out in consultation with core teams members by \*\*\*\*Speech and Language Therapy Org\*\*\*\* team. Bulk of programming of device/ maintain back-ups (\*\*\*\*Team Area ie. Fife\*\*\*\* \*\*\*\*Speech and Language Therapy Org\*\*\*\* Server), will move towards education staff once they are trained. Pass codes to allow editing and back ups are shared with key staff (Family, Education Staff and Speech Language Therapists), who will take on this role.
* When returned, device is wiped of programme and back-ups cleared

2.9 What Personal (PII)/Health Protected Information (PHI) will be used?

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Suppliers** | **\*\*\*\*NHS Scotland Health Board\*\*\*\*** | **Source** |
| **HCP** |  |  |  |
| Authority/Board | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Contractor name |  |  |  |
| Hospital name | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| First name | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Middle name |  |  |  |
| Last name | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Position | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Work Email | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Work Tel number | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| ***Carers*** |  |  |  |
| Authority/Board |  |  |  |
| Contractor name |  |  |  |
| Hospital name |  |  |  |
| First name | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Middle name |  |  |  |
| Last name | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Position | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Home address |  |  |  |
| Work address |  |  |  |
| Chat (Signal, WhatsApp etc.) |  |  |  |
| Email |  |  |  |
| Work Tel number | **⚫** |  | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Mobile Tel number (MFA) |  |  |  |
| **Patient** |  |  |  |
| First name | **⚫** | **⚫** | client/family/carers |
| Middle name | **⚫** | **⚫** | client/family/carers |
| Last name | **⚫** | **⚫** | client/family/carers |
| Date of birth | **⚫** | **⚫** | client/family/carers |
| Year of birth |  |  |  |
| Age | **⚫** | **⚫** | client/family/carers |
| Gender | **⚫** | **⚫** | client/family/carers |
| Home address | **⚫** | **⚫** | client/family/carers |
| Email | **⚫** | **⚫** | client/family/carers |
| Patient consent |  |  |  |
| **Family** |  |  |  |
| First name | **⚫** | **⚫** | client/family/carers |
| Middle name | **⚫** | **⚫** | client/family/carers |
| Last name | **⚫** | **⚫** | client/family/carers |
| Home address | **⚫** | **⚫** | client/family/carers |
| Relationship | **⚫** | **⚫** | client/family/carers |
| ***Friends*** |  |  |  |
| First name | **⚫** | **⚫** | client/family/carers |
| Middle name | **⚫** | **⚫** | client/family/carers |
| Last name | **⚫** | **⚫** | client/family/carers |
| Hobbies | **⚫** | **⚫** | client/family/carers |
| ***Other*** |  |  |  |
| Device Settings | **⚫** | **⚫** | \*\*\*\*Speech and Language Therapy Org\*\*\*\* |
| Devices (SMART phones, tablets etc.): | **⚫** | **⚫** | \*\*\*\*Speech and Language Therapy Org\*\*\*\* |
| IP address | **⚫** | **⚫** | \*\*\*\*Speech and Language Therapy Org\*\*\*\* |
| Device ID | **⚫** | **⚫** | \*\*\*\*Speech and Language Therapy Org\*\*\*\* |
| Passive information (status/error) |  |  | \*\*\*\*Speech and Language Therapy Org\*\*\*\* |
| Software License Terms and Conditions | **⚫** | **⚫** | \*\*\*\*Speech and Language Therapy Org\*\*\*\* |
| Software Use Agreements and Consents | **⚫** | **⚫** | \*\*\*\*Speech and Language Therapy Org\*\*\*\* |
| Software version and updates | **⚫** | **⚫** | \*\*\*\*Speech and Language Therapy Org\*\*\*\* |
| Security patches |  |  |  |
| Device (smartphone/tablet etc.) |  |  |  |
| Medical device registration information |  |  |  |
| Event Tracking |  |  |  |
| Monitoring (Growth, cardiac, medication) |  |  |  |
| Connectivity (WIFI, Bluetooth etc.) |  |  |  |
| Call history access |  |  |  |
| Web history access |  |  |  |
| Geolocation information |  |  |  |
| File storage access |  |  |  |
| Download access |  | **⚫** | \*\*\*\*NHS Scotland Health Board\*\*\*\* |
| Audio and video access |  |  |  |
| Accession # |  |  |  |
| Age |  |  |  |
| Gender |  |  |  |

Likely to hold health data so client can explain their needs and potential to hold financial data. (Financial data is not classed as special category in GDPR but the ICO treats financial data as special category due to the damage that can occur to an individual from a breach.) Provided by client/family/carers

2.10 Who will have access to the personal data?

The data owners using the AAC device can use this data to communicate with those around them. As many clients will require support in using /updating their device family members, support staff, teachers etc. will also be able to access the personal data of the individual user.

\*\*\*\*Speech and Language Therapy Org\*\*\*\* staff will have access to the data when working with the clients and to data backups. This is enforced by the GP/D3 Appendix 2 – (Attached in documents table)

\*\*\*\*Local Authority\*\*\*\* business support/server team maintenance will have access to data when required for maintenance purposes.

AAC device and programme providers (third parties) may have access to the data depending on the terms of use for the device or programme for troubleshooting issues, customer support & development only.

|  |  |  |  |
| --- | --- | --- | --- |
| Role | **Organisation** | **Level** | **Access** |
| IT Dept | \*\*\*\*Local Authority\*\*\*\* | Maintenance and Admin | ✓ |
| Install and Support Admin | X |
| Super User | X |
| User | X |
| View Only | X |
| Contractor IT | Liberator  Tobbi Dynavox  Smartbox | System Maintenance | ✓ |
| Support Admin | ✓ |
| Super User | X |
| User | X |
| View Only | X |
| \*\*\*\*Speech and Language Therapy Org\*\*\*\* | \*\*\*\*NHS Scotland Health Board\*\*\*\* | System Admin | X |
| Install and Support Admin | X |
| Super User | ✓ |
| User | ✓ |
| View Only | ✓ |
| Client | \*\*\*\*NHS Scotland Health Board\*\*\*\* | System Admin | X |
| Install and Support Admin | X |
| Super User | X |
| User | ✓ |
| View Only | x |

2.11 How will the information be collected, used, transferred and kept up-to-date?

Personalised vocabulary is collected from a variety of sources and is unique to each client. The primary source will generally be the client. However, where possible or required, family members, friends, carers and other support staff will contribute. It will depend on the client’s capacity and communication capability as to how much input they will have and the volume and content of information stored on the AAC device.

The information is collected via questionnaires and ongoing discussions/reviews with the client. The content on the AAC device is reviewed regularly and updated as required so it reflects the client’s communication needs. Backups of the client’s AAC devices are kept on a \*\*\*\*Speech and Language Therapy Org\*\*\*\* shared drive within the \*\*\*\*Speech and Language Therapy Org\*\*\*\* \*\*\*\*Local Authority\*\*\*\* Server. Information can also be transferred to the AAC device by an encrypted portable hard drive.

The type of data collected and method of storing the data is unique to each type of AAC device. See appendix 1 for a table of devices, they type of data they store and accessibility options.

2.12 Will the information be shared with any other organisation? Will it be used for research? If so, how?

Data is retained in \*\*\*\*Local Authority\*\*\*\* Servers – Sharing agreements are in place through the HSCP

Due to the nature of the AAC devices, the clients will be sharing the personal data within them when they use them to communicate. While it will not be all personal data held within the device, the decision to share this information will be made by the client and family support.

Some complex devices are under warranty with communication equipment suppliers. If device needs to be upgraded or repaired, access to information could be made by the third party working on device. This will be carried out with consent of the individual who has the device and recorded as such.

Some complex AAC devices and the application that are used are cloud based. Therefore the personal data will be processed by an external data processor, recorded above. Where this is the case, the contract and terms & conditions will be checked for UK GDPR and Data Protection Act compliance.

If the app or device does not connect to the internet and only uses information stored on the device then the data processor is \*\*\*\*Speech and Language Therapy Org\*\*\*\* and \*\*\*\*Local Authority\*\*\*\* for the storage of the data within their environment.

2.13 What are your data retention periods?

|  |  |  |
| --- | --- | --- |
| Organisation | **Data Type** | **Minimum Retention Period** |
| \*\*\*\*NHS Scotland Health Board\*\*\*\* | As described. | As per Scottish Government Records Management Policy. |
| \*\*\*\*Local Authority\*\*\*\* |  |  |

The personal data will be kept for as long as the data owner requires the AAC device.

\*\*\*\*NHS Scotland Health Board\*\*\*\* -Management, Retention, Storage and Destruction of all Business and Administrative Information and Records and \*\*\*\*NHS Scotland Health Board\*\*\*\* - Health Records Retention and Destruction detailing the minimum retention period for the information and procedures for the safe disposal of personal information.

\*\*\*\*Local Authority\*\*\*\* Cloud Services are being used for the storage – retention periods will be in line with their retention polices. A copy of their policy is attached in the documents table.

Liberator - None of our devices require connection to the internet to operate as solely communication aids. Customers may wish to connect to the internet to access ‘other’ apps, social media platforms etc. In such instances, it is the customer’s responsibility to ensure adequate security.

Tobii Dynavox (ISPP Document Extract)

* 1. Retention
     1. Private and sensitive information is not stored longer than needed. Additional consideration may be given to data meeting the following qualifying conditions:
        1. HIPAA and Medicare data will follow CMS retention policies
        2. FERPA will follow DOE retention policies
        3. Data subject to GDPR will follow GDPR Data retention policies
        4. Non-client-specific data will be disposed of securely when no longer needed for legal, regulatory, or other business reasons.
     2. All information required to be returned to a client will be done so following the appropriately secure method for the transport (secure FTP, encrypted media, etc.).
     3. Traffic and device logs are stored for ninety (90) days. Summarized traffic and device logs, syslog information, and auditing information, is saved for one (1) year where possible.
  2. Physical Disposal
     1. Paper content, or other non-electronic physical media, that contains sensitive information, including private or sensitive data, is disposed of in a proper fashion (shredded with cross-cut) when it is no longer required for business or service purposes.
  3. Electronic Disposal
     1. Electronic media containing sensitive or private data and information, is disposed of in the proper fashion. Depending on the media, and whether it will be reused, it will be deleted/wiped, or destroyed following NIST guidelines.
     2. If a third-party vendor is used to securely destroy media, the destruction will be validated by a member of management, or the appropriate certification will be acquired.
     3. When technology assets have reached the end of their useful life, or transitioned to secondary production use, they will be wiped (have data deleted) following appropriate NIST guidelines, then deposed of if not being repurposed.

Smartbox (Privacy Policy Extract)

**The length of time we keep your data**

We only keep your personal data for as long as necessary.

**Information taken to generate or fulfil a quote, or carry out a visit**

We are legally obliged to keep your Order information for seven years. We also keep visit

information for seven years, to comply with regulations.

**Smartbox Account**

If you create a Smartbox Account, we will only keep your data for 12 months after the account becomes inactive.

**Smartbox Newsletter**

We will keep you on our mailing lists for as long as you continue to show interest in Smartbox.

Your data will be stored for 18 months after your last opened email.

**Smartbox Support**

If you contact our Support Team using the Online Chat service, conversations will be

recorded for 12 months.

**Repair services**

During any repair procedures, with your consent, we keep backups of device data for up to

three months. We will keep details and notes of support tickets and repairs for up to seven

years, for legal purposes.

**Website forms**

Any form submitted to the website is stored for a maximum of 60 days.

2.14 Will the information be moved, accessed or shared offshore?

Some complex AAC devices and the application that are used are cloud based, therefore the personal data will be processed by an external data processor and could therefore the information could leave the EEA. Each device and application will need to be reviewed to determine if safeguards are required for the personal data being processed.

2.15 What is the legal basis for using personal data?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Processing of Personal Information** | | | **Processing of Special Category Information** | | |
| **Law** | **Basis** | **✓** | **Law** | **Basis** | **✓** |
| 6(1)(a) | **Consent of the data subject.** | **✓** | 9(2)(a) | **Explicit consent of the data subject unless reliance on consent is prohibited by UK law.** | **✓** |
| 6(1)(b) | Processing is necessary for the performance of a contract. |  | 9(2)(b) | Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement. |  |
| 6(1)(c) | Processing is necessary for compliance with a legal obligation. |  | 9(2)(c) | Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent. |  |
| 6(1)(d) | Processing is necessary to protect the vital interests of a data subject. |  | 9(2)(d) | Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union provided the processing relates only to members or former members and there is no disclosure to a third party without consent. |  |
| **6(1)(e)** | **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.** | **✓** | 9(2)(e) | Processing relates to personal data manifestly made public by the data subject. |  |
| 6(1)(f ) | Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party. |  | 9(2)(f) | Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity. |  |
|  | | | 9(2)(g) | Processing is necessary for reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued and which contains appropriate safeguards. |  |
| **9(2)(h)** | **Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis UK law or a contract with a health professional**. | **✓** |
| 9(2)(i) | Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices. |  |
| 9(2)(j) | Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1). |  |
| **Health (Tobacco, Nicotine etc. and Care) (Scotland) Act 2016** | | | **✓** |  |  |
|  | | |  |  |  |
|  | | |  |  |  |
|  | | |  |  |  |

2.16 How will people's information and privacy rights be protected?

|  |  |  |
| --- | --- | --- |
| **UK GDPR Rights** | **Guidance** | **Applicant Response** |
| **Right of Access** | Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is called a Subject Access Request (SAR). You should respond within one month of receipt of a SAR. All information relating to a SAR should be managed and disclosed securely. | Individuals may request this data through their Board who will in turn obtain the patient information from the Prime Contractor, sub-contractors or through NHS. All supply chain partners will work collaboratively to respond to such requests for in a timely manner. This is also a contractual obligation.. |
| **Right to Rectification** | The UK GDPR includes a right for individuals to have inaccurate personal data rectified and complete. You have one month to respond to a request. | Individuals may request this data through their Board who will in turn obtain the patients information from the Prime Contractor, sub-contractors or through NHS. All supply chain partners will work collaboratively to respond to such requests in a timely manner. This is also a contractual obligation.. |
| **Right to Object** | The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. You must inform individuals about their right to object. | This right will be communicated to all Data Subjects. The right may not apply where the clinical pathway of the patient would be compromised. The Boards will not always accede to them e.g. if they have compelling overriding legitimate grounds to continue processing. |
| **Right to Restrict Processing** | Individuals have the right to request the restriction or suppression of their personal data. | This is not an absolute right and only applies in certain circumstances. For example, this may not apply where the clinical pathway of the patient would be compromised. |
| **Right to Data Portability** | The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. | This right is only available where the legal basis for processing under the GDPR is consent, or for the purposes of a contract between participating patients and NHS. |
| **Right to Erasure** | The UK GDPR includes a right for individuals to have personal data erased. The right to erasure is also known as ‘the right to be forgotten’. | This may not apply where the clinical pathway of the patient would be compromised. This is a contractual commitment. The Contractor shall promptly comply with any Written request from the Authority requiring the Contractor to amend, transfer or delete the Personal Data. |
| **Rights in Relation to Automated Decision-making and profiling** | As systems and technology evolve it is important to understand automation use, especially at core system level, and the degrees of human control and intervention. The UK GDPR applies to all automated, individual decision-making and profiling. | The is no automated decision-making in this process without human intervention. |

1.17 What information is being provided to people to whom the data relates to ensure they are aware of this use of their personal data?

A basic requirement of Data Protection Law is that individuals should be told who is holding their information, what the Data Controller intends to do with the information and who else they may share it with. For the purposes of the review processes all Parties are Data Controllers of the Personal Data they hold, including Data that they receive from each other.

Each Party must ensure that they have appropriate policies and procedures in place to facilitate both the protection and the exercising of rights of individuals under Data Protection Law. Each Party will comply with the rights of the individuals in a fair and consistent manner and in accordance with any specific legislative requirements, regulations or guidance.

\*\*\*\*NHS Scotland Health Board\*\*\*\* will inform their patients/clients/service users about the use of PII data. This will be achieved through patient information leaflets, posters and web pages.

\*\*\*\*NHS Scotland Health Board\*\*\*\* has Fair Processing / Privacy Notices and inform patients / public about the use of data through leaflets such as “Confidentiality: Your Rights” and “How the NHS Handles your Personal Health Information”. The \*\*\*\*NHS Scotland Health Board\*\*\*\* Privacy Notice is available at: \*\*\*\*Health Board Privacy Notice Link\*\*\*\*

Additional information is also available via the NHS Inform website:

<https://www.nhsinform.scot/care-support-and-rights/health-rights/patients-charter/the-charter-of-patient-rights-and-responsibilities>

<https://www.nhsinform.scot/publications/confidentiality-your-rights-factsheet>

<https://www.nhsinform.scot/publications/how-the-nhs-handles-your-personal-health-information-leaflet>

The \*\*\*\*NHS Scotland Health Board\*\*\*\*, \*\*\*\*Local Authority\*\*\*\*, Tobii Dynavox, Liberator and Smartbox Privacy Policies are attached in the document table.

1.18 Who have you consulted with about this project?

|  |  |  |
| --- | --- | --- |
| **Name** | **Position** | **Email** |

6.0 ORGANISATIONAL AND TECHNICAL CONTROLS

\*\*\*\*NHS Scotland Health Board\*\*\*\* and \*\*\*\*Local Authority\*\*\*\*

| **Type of Control – examples** | **Description** |
| --- | --- |
| Information security and related policy(ies) | **\*\*\*\*NHS Scotland Health Board\*\*\*\*:**   * GP/A4 Acceptable Use Policy * GP/C10 Clear Desk Clear Screen Policy * GP/D3 * GP/I5 \*\*\*\*NHS Scotland Health Board\*\*\*\* Information Security Policy * GP/P2 Password Policy * GP/I6 IT Change Management Policy * GP/M4 Media Handling Policy * GP/V2 Virus protection Policy   **\*\*\*\*Local Authority\*\*\*\***  Policies in place |
| Staff training | \*\*\*\*NHS Scotland Health Board\*\*\*\*:  All Staff sign confidentiality agreements  All staff undertake 3 yearly in house core training and complete 2 yearly Information Governance LearnPro module (\*\*\*\*NHS Scotland Health Board\*\*\*\* Information Governance 2017).  All mandatory training is monitored regularly.  Team members are given training on the software uploading, other aspects of assistance.  **Supplier**  \*\*\*\*Local Authority\*\*\*\*  All staff members carry out information governance training. |
| Adverse event reporting and management | \*\*\*\*NHS Scotland Health Board\*\*\*\*:   * GP/I5 Information Security Policy * GP/S8 eHealth Incident Management Policy   **\*\*\*\*Local Authority\*\*\*\***  Have Policies in place |
| Physical access and authorisation controls | \*\*\*\*NHS Scotland Health Board\*\*\*\*:   * GP/A4 Acceptable Use Policy * GP/I5 \*\*\*\*NHS Scotland Health Board\*\*\*\* Information Security Policy * GP/D4 Appendix 2 – \*\*\*\*NHS Scotland Health Board\*\*\*\* IG Structure, Role and Responsibilities   **\*\*\*\*Local Authority\*\*\*\***  Have Policies in place |
| Environmental controls | \*\*\*\*NHS Scotland Health Board\*\*\*\*:   * GP/I5 \*\*\*\*NHS Scotland Health Board\*\*\*\* Information Security Policy   **\*\*\*\*Local Authority\*\*\*\***  Have Policies in place |
| Information asset management including management of backups and asset disposal | \*\*\*\*NHS Scotland Health Board\*\*\*\*:   * GP/I6 eHealth Change Management Policy * eHealth Back up * Hardware Condemnation Procedure   **\*\*\*\*Local Authority\*\*\*\***  Have Policies in place |
| Business continuity | \*\*\*\*NHS Scotland Health Board\*\*\*\*:   * GP/I5 \*\*\*\*NHS Scotland Health Board\*\*\*\* Information Security * eHealth BC and DR Operational Procedures * eHealth Infrastructure BC and DR Framework Plan   **\*\*\*\*Local Authority\*\*\*\***  Have Policies in place |
| Data Backup | \*\*\*\*NHS Scotland Health Board\*\*\*\* uses Netapp Snapshots to back up its data. It also uses cross site copying to allow system failover to take place in a disaster scenario.  GP Practices currently use tape backup for their data.  \*\*\*\*Speech and Language Therapy Org\*\*\*\* – encrypted portable devices  **\*\*\*\*Local Authority\*\*\*\***  Have Policies in place |
| *Add others where applicable* | ***Microsoft Limited - Z6296785***  <https://ico.org.uk/ESDWebPages/Entry/Z6296785>  **\*\*\*\*Local Authority\*\*\*\* – ICO Registration** |

Tobii Dynavox

| **Type of Control – examples** | **Description** |
| --- | --- |
| Information security and related policy(ies) | **Tobii Dynavox**  See attached Tobii Dynavox ISPP.docx |
| Staff training | **Tobii Dynavox**  See attached *Boardmaker7-Organization-Security-whitepaper.pdf* |
| Adverse event reporting and management | **Tobii Dynavox**  Attempts at unauthorized access to our secure databases are reported to administrators. Vulnerability reports are ran regularly and reviewed. |
| Physical access and authorisation controls | Tobbi Dynavox - Boardmaker 7 is hosted on the Azure platform which is a globally distributed network of datacenters. Physical access to these datacenters have multiple layers of security managed by Microsoft |
| Environmental controls | Tobii Dynavox - Microsoft datacenters are protected from environmental hazards through climate control, fire detection & suppression and water sensors |
| Information asset management including management of backups and asset disposal | Tobii Dynavox - SQL Databases hosted by Microsoft Azure are configured with the following backup and retention policies. The preservation & disposal of each backup is managed by Microsoft.  Tobii Dynavox has confirmed that any personal data collected for the registration of accounts is stored in servers located in Canada only. The data is never transferred after creation. Canada has an adequacy decision regarding commercial companies. |
| Business continuity  Data Backup | Tobii Dynavox - SQL Databases hosted by Microsoft Azure are configured with the following backup and retention policies. The preservation & disposal of each backup is managed by Microsoft.  Differential backups of the database are taken every 12-24 hours and preserved for 21 days. Transaction logs are backed up every 5-10 minutes. These allow the database to be restored to instant during the retention period.  Full backups are taken once a week and preserved up to 4 weeks. At the end of each retention period, backups and all their data are disposed.  <https://goboardmaker.com/pages/terms-and-conditions> |
| System access levels and user authentication controls | **Tobii Dynavox**  Boardmaker 7 Organization software, communication and database servers are hosted in the Microsoft Azure Cloud, which is a highly secured Tier 1 data center. Physical access to servers is not allowed. Search services are currently provided by Elastic Search, which has similar facility security.  Permissions are granted to staff with a need for access by using role-based access control with Active Directory. Boardmaker 7 Organization software, communication and database servers are hosted in the Microsoft Azure Cloud, which is a highly secured Tier 1 data center. Physical access to servers is not allowed. Search services are currently provided by Elastic Search, which has similar facility security. |
| System auditing functionality and procedures | **Tobbi Dynavox**  All databases containing personal information have an audit trail of access & changes. Tobii Dynavox’s approach to security and privacy is simple: Start with a secure hosted service and operational practices that preserve customer privacy. Protect data connections with authentication and state-of-the-art encryption to keep traffic safe. Integrate this solution seamlessly with each district’s existing network and security infrastructure. Provide flexible administrative controls for user management. The end result: Boardmaker 7 Organization is a robust, secure education management and delivery system with low total cost of implementation (TCI).  Tobii Dynavox’s approach to security and privacy is simple: Start with a secure hosted service and operational practices that preserve customer privacy. Protect data connections with authentication and state-of-the-art encryption to keep traffic safe. Integrate this solution seamlessly with each district’s existing network and security infrastructure. Provide flexible administrative controls for user management. The end result: Boardmaker 7 Organization is a robust, secure education management and delivery system with low total cost of implementation (TCI). |
| Operating system controls such as vulnerability scanning and anti-virus/anti-malware software | **Tobbi Dynavox**  Vulnerability scanning and anti-virus protection is handled by Microsoft. All Azure software components undergo a virus scan by Microsoft Endpoint Protection.  **Protecting confidential data**  Boardmaker 7 Organization uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the user’s browser and the server is protected with end-to-end 256-bit RSA encryption. We use a Premium SSL wildcard certificate.  **Password Protection**  Any system that allows users to login can be compromised by using weak passwords that can easily be guessed, or by sharing passwords. Boardmaker Online enforces a minimum password length of 6 characters, and it does display password strength when users are creating or changing their passwords. |
| Network security such as firewalls and penetration testing | Tobbi Dynavox  Access to all personal data is protected by a server level firewall. Boardmaker 7 Organization is firewall friendly. It generates only outgoing HTTP/TCP to ports 80, 443. Because most firewalls are already configured to permit outgoing Web traffic, you do not have to bypass or compromise your district or location firewall. |
| Encryption of special category personal data | **Tobbi Dynavox**  All data, regardless of category, is encrypted at rest using 2048-bit RSA. In transit, TLS 1.2 is required for all data. |
| Cyber Essentials compliance(if applicable) | Tobbi Dynavox  See ISPP |
| System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available) | Tobbi Dynavox  See ISP in Documents Table |
| Details of ISO27001/02 accreditation and scope (if applicable) | Tobbi Dynavox |
| *Add others where applicable* | Tobbi Dynavox  See security paper in Documents Table |

**Liberator – Have given the supplied device controls.**

| **Type of Control – examples** | **Description** |
| --- | --- |
| System access levels and user authentication controls | Our Windows, Android and IOS based communication aids are sold with no passwords as they are non-personalised at the point of sale. The customer/user may wish to add a password, add a pin, or use biometric recognition to access these devices on start-up in much the same way as one would a personal pc or tablet. |
| System auditing functionality and procedures | It will be the responsibility of the device owner to monitor the device; However, Liberator offer technical support and repairs on devices as and when required. |
| Operating system controls such as vulnerability scanning and anti-virus/anti-malware software | Windows based devices are supplied with Windows 10 (updated to the latest version at point of sale) with all features of the Microsoft Defender Antivirus turned on. Customers may wish to |
| Network security such as firewalls and penetration testing | None of our devices require connection to the internet to operate as solely communication aids. Customers may wish to connect to the internet to access ‘other’ apps, social media platforms etc. In such instances, it is the customer’s responsibility to ensure adequate security. |
| Encryption of special category personal data | Liberator do not store any information within their CRM system or servers about a person’s health status, race, religion, ethnic origin or any special category data etc.  However, customers at times ask that Liberator retains their saved communication vocabulary. In such instances, these are stored in our secure servers with the consent of the customer. Such data may contain personal details of the customer, stored by the customer. Generall |
| Cyber Essentials compliance (headers  if applicable) | No, Liberator does not have Cyber Essentials compliance. |
| System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available) | Liberator is an ISO 9001 accredited company so all of our procedures are documented. |
| Details of ISO27001/02 accreditation and scope (if applicable) | ISO 9001 accredited company |
| *Add others where applicable* | ICO |

**Smartbox**

| **Type of Control – examples** | **Description** |
| --- | --- |
| Information security and related policy(ies) | Polices are in place.   * Corporate and systems policies have been developed with Cybersecurity controls integrated into the design. yes * The prescribed controls are based on: Cyber Essentials plus Accreditation * UK DPA/GDPR 2018 Yes * Data Privacy Policy in place. Yes * Cyber Essentials Plus accreditation. Yes * Contractor and sub-contractors will adhere to all applicable data protection, security and privacy regulations and laws. Yes |
| Staff training | Training is provided on a regular basis to personnel and customers.   The training includes annual data security and privacy. |
| Adverse event reporting and management | Smartbox prides itself in the quality of its solutions and support  Smartbox acknowledges that the requirements of this DPIA and any Agreement are a moral minimum and will respond immediately should an adverse event occur |
| Physical access and authorisation controls | * All physical access and authorisation to internal administration systems and health care platforms is controlled through Conditional Access and Least Privilege. * Employee and contractor activity is monitored. * All Smartbox buildings are secured with appropriate security, access control, theft alarms. and CCTV. |
| Environmental controls | All Smartbox buildings are secured with appropriate security, access control, theft alarms. and CCTV.  Access to secure areas is controlled. |
| Information asset management including management of backups and asset disposal | * A routine daily and weekly back-up schedule is maintained. * When a device reaches end of life, it is returned to the IT Department and securely destroyed, including all data. * When a device is being made ready for re-use or decommissioned, the first step is that all data is securely destroyed. Yes all devices are wiped before use or destroyed when end of life * All data assets are securely destroyed.  Yes |
| Business continuity  Data Backup | Information management is managed through…   * Yes - A routine daily and weekly back-up schedule is maintained. * Yes - When a device is being made ready for re-use or decommissioned, the first step is that all data is securely destroyed. * Yes - All data assets are securely destroyed. * Policy, process and procedures defining Business Continuity/Disaster Recovery (BC/DR) are in place to minimize the impact of a realized risk event. |
| System access levels and user authentication controls | * Yes, Mobile devices are secured and monitored. * MFA is enabled on all systems where possible * Users are automatically locked out of their account if they enter incorrect login information 5 times or after a 30 minute period of inactivity. Azure account lockout policy in place. * User activities are logged and monitored -Yes account login activity logged |
| System auditing functionality and procedures | MS Windows update and Smartbox update to ensure latest security updates and bug fixes/features are added. |
| Operating system controls such as vulnerability scanning and anti-virus/anti-malware software | Device - Installed on all Smartbox AAC devices (Microsoft Defender). Responsibility to update and scan lies with the user/customer  **Platform-**   * Yes - Threat assessment includes both vulnerability and penetration testing elements. * Yes - Vulnerability Assessments are performed weekly. – Currently carried out annually as part of pen testing * Yes - A cybersecurity assessment (e.g. penetration test) is performed annually. * The connectivity platform requires at least annual certification of entitlements for all system users and administrators. Yes, all accounts are renewed on an annual schedule. * Yes - The platform has an identity management system in place which enables both role-based and context-based entitlement to data. There are Role based access in place for all systems * Policy, process and procedures defining Business Continuity/Disaster Recovery (BC/DR) are in place to minimize the impact of a realized risk event. |
| Network security such as firewalls and penetration testing | * A regular schedule of logs, patching and updates is maintained.  A weekly patch schedule takes place for all devices with Servers patched on a monthly cycle. * Development and testing takes place in a non-production environment.  yes * A register of asset IDs is maintained. All assets are identified and tagged. All assets are assigned an Owner * All device details are maintained and recorded in the asset register and assigned an owner and retired when no longer in use * All Third Party service providers/sub contractors are selected on the basis of their demonstrable commitment to cybersecurity and data privacy. |
| Encryption of special category personal data | Smartbox do not encrypt or password protect the AAC device. This is the responsibility of the user/customer. Both can prevent user access as password screens are inaccessible to most alternative access methods.  **Platform**   * All data - AES-256-bit encryption algorithm. * TLS/HTTPS |
| Cyber Essentials compliance(if applicable) | * The prescribed controls are based on: Cyber Essentials plus Accreditation * Cyber Essentials Plus accreditation. Yes |
| System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available) | * Yes, Corporate and systems policies have been developed with Cybersecurity controls integrated into the design. |
| Details of ISO27001/02 accreditation and scope (if applicable) |  |
| *Data Centres* | * Data is retained in UK Datacenters (Grid Software – Dropbox GDPR compliant but data centres are not confirmed to be in the UK) * Yes, all data at rest and in motion is encrypted. |
| Support | * L0 - (UK) Self-help. * L1 - (UK) Help desk. No access to treatment files, only basic patient information. * L2 - (UK) Technical support. No access to treatment files, only basic patient information. * L3 - (UK) Expert support. Only when required for trouble shooting advanced technical issues with the patient device, Will have access to specific treatment files from a specific patient.   No access to treatment files unless provided by \*\*\*\*NHS Scotland Health Board\*\*\*\* |

7.0 DOCUMENTATION TABLE

Please e-mail [dhac@gov.scot](mailto:dhac@gov.scot) to receive relevant table.

8.0 PRINCIPLES ASSESSMENT

What level of risk has been identified in relation to the following Data Protection Principles?

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Protection Principles** | **Low** | **Medium** | **High** |
| Personal and health data is processed in a fair, lawful and transparent manner. | ✓ |  |  |
| Personal and health data is collected for specific, explicit and legitimate purposes. | ✓ |  |  |
| Personal and health data is adequate, relevant and limited to what is necessary. | ✓ |  |  |
| Personal and health data is accurate and kept up to date. | ✓ |  |  |
| Personal and health data is kept no longer than necessary. | ✓ |  |  |
| Personal and health data is processed in a manner that ensures adequate security. | ✓ |  |  |

9.0 RISK ASSESSMENT

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood (L)** | **Score** | **Consequence (C)** | **Score** | **Final Score** | **Condition** |
| Remote | 1 | Negligible | 1 | 0 - 20 | Negligible |
| Unlikely | 2 | Minor | 2 | 21 - 40 | Minor |
| Possible | 4 | Moderate | 4 | 41 - 60 | Moderate |
| Likely | 8 | Major | 8 | 61 - 80 | Major |
| Certain | 10 | Extreme | 10 | 81- 100 | Extreme |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk #** | **Description** | **L** | **C** | **R** | **Mitigation/ Actions** | **Residual Risk** | **Risk Owners** | **Date** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

10.0 ACCEPTANCE

|  |  |  |
| --- | --- | --- |
| **Role** | **Advice/ Action/ Sign-Off** | **Date** |
| IG/ Data Protection (DPO) Advice |  |  |
| Information Security Officer Advice (questions 11 and 12) |  |  |
| Caldicott Guardian, |  |  |
| DPO opinion on whether residual risks need prior notification to the ICO |  |  |
| Information Asset Owner(s) (IAO(s)) Sign Off |  |  |

**The next review date for this DPIA will be in \_\_\_\_\_ months from date of approval.**

1. APPENDICES

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Device Type | Provider | Personal Data | Data Format | Data Location |
| *Device name* | *App, audio device, tablet etc.* | *Provider Name* | *Type of personal data e.g. name, number, medical etc.* | *Text, audio, pictures etc.* | *Cloud, device etc.* |
| Grid Pad 12/13 | Windows 10 Device with specialist communication software – grid 3 | Smartbox Assistive Technology | Name/contacts/personalised vocabulary/email/phone contacts/stored phrases | Text/audio/photos | Stored on device and cloud |
| Indie | Windows device with specialist communication software – snap n core | Tobbii Dynavox | Name/contacts/personalised vocabulary/email/phone contacts/stored phrases | Text/audio/photos | Stored on device and cloud |
| Ipads and minis with specialist communication software | Tablet with  Apps –  Grid 3  Snap n core  Predictable  Assistive express  Go Talk  Clicker  Proloquo2go  Pecs | Apple | Dependant on specialist communication app installed but generally storing personalised vocabulary/photos/contacts/stored phrases. Device also  affords use of social mediaemail/texting/  whatsapp/facebook/ | Text/audio/symbol  /photos | On device  Back up to cloud on some apps  Use of personalised dropbox account for client data also used on go talk app. |

**The device specific Dropbox account set up for the client will only be used to backup the client data in the event of a loss of their programmes and deployment of new programmes for the client.**