Data protection policy- Growing Hope

1. Aims

Growing Hope aims to ensure that all personal data collected about families, trustees, staff, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Responsible individuals

- Trustees of national charity and local charity.
- Clinic Managers
- Other volunteers and individuals working as part of Growing Hope clinics.

Non-disclosure agreement (NDA) needs to be signed by all individuals to confirm that they will not use any personal data for purposes other than those explicitly agreed with Growing Hope to fulfil role responsibilities (www.growinghope.org.uk/non-disclosure-agreement).

3. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials)

	• Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Growing Hope (national CIO) and Growing Hope local clinics (local CIO's) process personal data relating to families, trustees, staff, visitors and others, and therefore are data controllers.

As not-for-profit organisations, Growing Hope CIO's are exempt from registering and paying the ICO as data controllers.

5. Roles and responsibilities

This policy applies to **all staff** employed by Growing Hope, and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. Volunteers and freelancers who do not comply with this policy may be asked to step down from their roles.

5.1 Growing Hope Trustees

Growing Hope Trustees have overall responsibility for ensuring that all Growing Hope clinics comply with all relevant data protection obligations.

5.2 Data Protection Officer

The data protection officer (DPO) is responsible for providing advice and guidance to the local Growing Hope clinics in order to assist them in implementing this policy and monitoring compliance with data protection law.

The DPO will carry out an annual review of data protection procedures across Growing Hope local clinics in order to ensure this policy is being adequately followed.

The DPO is: Paul Nye, paul.nye@growinghope.org.uk / 07496528506

5.3 All staff and volunteers

All members of staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the charity of any changes to their personal data, such as a change of address
- Contacting the designated Data Protection Officer in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on data protection principles that Growing Hope (CIOs) must comply with. Growing Hope has adopted these principles to underpin its Data Protection Policy:

The principles require that all personal data shall be:

(1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

(2) used for specified, explicit and legitimate purposes ('purpose limitation');

(3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');

(5) kept no longer than is necessary ('storage limitation');

(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

This policy sets out how Growing Hope aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Growing Hope shall only process personal data where it has one of 5 'lawful bases' (legal reasons) available under data protection law:

- The data needs to be processed so that Growing Hope can **fulfil a contract** with the individual, or the individual has asked the Clinic to take specific steps before entering into a contract
- The data needs to be processed so that Growing Hope can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that Growing Hope can perform a task **in the public interest,** and carry out its official functions
- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear **consent**

For special category data (health information) we follow the following lawful reasons when collecting data:

- Gaining **explicit consent** for the data we collect
- We process health care data in order to run our therapy clinics- this is considered a **legitimate activity with appropriate safeguards by a not-for-profit body with a religious aim.**
- We process data as **necessary for preventive medicine** in order to form appropriate clinical assessment and intervention.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff and volunteers must only process personal data where it is necessary in order to do their jobs.

When staff or volunteers no longer need the personal data they hold, they must ensure it is deleted or anonymised as per the data-mapping section at the end of this policy.

7.3 Data Gathering

We will collect the data that individuals share when communicating with us. This could be in the course of making a donation or signing up to an email newsletter. However, we won't search for data such as personal telephone numbers or email addresses if individuals haven't supplied them to us.

We may also receive data about individuals when they interact with third parties with whom we work, for example, but not limited to, if they've made a donation to us through a third-party website (such as JustGiving) and given them permission to share their data with us.

We also collect general information about visitors to our website using cookies, including which web pages they look at and for how long. This helps us make our website better and more relevant for visitors. This information is anonymous and cannot be used to identify people. We take a similar approach with the emails we send, tracking how many are opened, and how many people click through to our website.

8. Sharing personal data

We refrain from sharing personal data to third parties where possible. However, GDPR and the DPA 2018 allow information to be shared where:

- There is an agreed reason for sharing data which is detailed within the collaboration agreement between Growing Hope, the church and the local Growing Hope charity.
- There is a safeguarding reason that puts a child, family or staff member at risk (as per our safeguarding policy).
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our families – for example, but not limited to, IT, Finance and HR companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of the families that we work with or staff.

When we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Clinic holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the Data Protection Officer – Paul Nye – paul.nye@growinghope.org.uk or 390 Calendonian Road, London, N1 0DH. They should include:

- Name of individual
- Name of the local Growing Hope
- Correspondence address
- Contact number and email address
- Details of the information requested

The DPO will send the subject access request to the Clinic Manager for that clinic. If staff receive a subject access request they must immediately ensure that the DPO is informed.

Information to be released will be collated by the Clinic Manager and then sent to the DPO for checking and sending out to the applicant.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for young people in clinic aged 13 and above may not be granted without the express permission of the young person.

For all Clinics:

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for children in clinic [aged under 13] will in general be granted without requiring the express permission of the child.

These are not fixed rules and a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to Clinic closure. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where processing is based on the consent of the child or parent
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff or volunteers receive such a request, they must immediately forward it to the Clinic Manager who will forward it to the DPO.

10. Data protection by design and default

Growing Hope will ensure that data protection is considered in its processes through the following:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the Clinic's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Annual training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our local clinics and DPO and all information we are required to share about how we use and process their personal data.
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

11. Data security and storage of records

Growing Hope will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. Please see the data mapping section below for an outline of how data is used, stored and destroyed.

12. Personal data breaches

Growing Hope will take all reasonable steps to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the steps as advised by the ICO to understand the severity of the breach and the action needed.

When appropriate, and following discussion with the DPO, the local Growing Hope shall report the data breach to the ICO within 72 hours. Such breaches in a Growing Hope context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a Growing Hope laptop containing non-encrypted personal data about children and families
- The loss of a piece of paper or diary containing personal information.

13. Training

All staff and trustees are provided with data protection training as part of their induction process and on an annual basis.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or Growing Hope's processes make it necessary.

14. Telephone calls

- Growing Hope will ask all staff to ensure that they are speaking with the correct person/ client by verifying their details. It may be appropriate to call them back to verify their credentials.
- If it becomes necessary to leave the phone for any reason, the staff member should put the caller on hold so that they cannot hear other potentially confidential conversations that may be going on in the office.
- If the call received or being made is of a confidential or sensitive nature, the staff member should consider who else may be listening to the conversation.
- If a message needs to be taken and left on someone's desk, staff members will ensure that these messages do not themselves contain confidential information.
- Staff members will be asked not to leave confidential messages on an answer machine as these can be reviewed by people other than the intended person.
- Telephone calls made to supporters or potential clinic partners may be recorded within Salesforce to track and follow supporter or partner journeys.

15. Conversations

- Staff should remember that even though they may be in clinic or a church office there may be visitors around.
- When having a meeting or interview with someone where confidential information will be discussed, ensure that there is sufficient privacy. Check that the room is suitable.
- Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job.
- Always consider your surroundings and the proximity of others who may be able to hear in public places.
- Parents and others who do not want to discuss their private matters with a member of staff in a public area should be offered the opportunity to be seen elsewhere

16. Information sharing/processing

When confidential or personal data is shared with other agencies, for example with local authorities or external providers, then arrangements must be made for that information

sharing to be done in a controlled way that meets ethical and legal obligations in one of two ways:

1. If a service is commissioned with an external provider that needs confidential information to operate then the contract must contain clauses that list the commissioned organisation's responsibilities for confidential and personal data, including data protection and security. This must include whether the organisation is processing personal data on behalf Growing Hope or has sole or joint responsibilities for the personal data with Growing Hope. All staff involved in such data commissioning/sharing must be aware of the details of any existing information sharing agreements/contractual agreements and the obligations that it places on them.

2. If information has to be shared with another organisation on a regular basis for legal reasons then this should be done under an information sharing agreement that sets out how the sharing will operate and the standards of management that all parties to the agreement must comply with. Such an agreement will define exactly what information will be shared and how, including the method, transmission or communication between agencies or any shared access security arrangements. The aim is to ensure that appropriate arrangements operate in the participant agencies and ensure the continued confidentiality of shared information. If staff are unclear on what basis information is being shared with another agency, whether an information agreement exists and what obligations that might place on them, it should be clarified with their manager.

17. Consent

- Growing Hope staff will ensure that all electronic google consent forms and feedback forms are stored securely within the G Drive. Any information pertaining to children will be stored within Canopy.
- Staff will ensure that written consent for photographs and video footage of children and families is obtained and uploaded to the G Drive where it can be stored securely.
- No member of staff should take recordings or photos without additional verbal agreement of a child/young person and their parents.

18. Customer Resource Management Tools

- Growing Hope are currently using a number of CRM tools to support our daily work including Sales Force, Quickbooks, Mail Chimp and other data collection avenues.

- As part of the security protocol for using these systems, Growing Hope National staff can access the entire databases, however local clinic managers and staff can only access data in relation to their own individual clinics.
- Supports will need to opt in to agree for us to record their information within our database.
- Upon doing so, we will ensure that the data Is encrypted and stored in line with GDPR protocols.
- If a support requests that their information is deleted, Growing Hope will ensure that this is completed and they are notified accordingly.

19. Working Away from Clinic

The purpose of this section is to ensure that information assets and information processing facilities, used to access personal and confidential information, are adequately protected with logical, physical and environmental controls.

This includes working away from the clinic, at home and use of own devices to access personal and confidential information.

Work-related information must not be kept permanently at home. Wherever staff are working on, or in possession of, work-related information they are responsible for it, e.g. in clinic, on the phone, at home, en route to or from clinic or home, at meetings, conferences, etc. If confidential information is handed out in conferences or meetings, the same person is responsible for collecting it back in at the end, or ensuring it is only in the hands of those authorised to keep it.

- Take only the confidential papers/files with you that you need and keep out of sight in a bag, do not carry around loose or in a clear folder.
- Store confidential paper files/records securely when out of the office. Try to use electronic files on an encrypted device or access via secure connection to the network or approved storage location instead.
- Keeping information in cars: lock away paper files and equipment (laptop/notebook) in the boot, do not leave overnight.
- Travelling by public transport: make sure you take all information and equipment when leaving. Be aware of conversations on mobile phones about personal and confidential information.
- Use of Laptops: If using a spreadsheet or system to store passwords, please ensure the system is encrypted and password protected. All files and work must

always be stored on Google Drive. When working on any Growing Hope Work, this should be stored within the relevant themed file.

- Working at home: Store paper and equipment securely after use, as you would your own personal valuables. Don't leave open confidential files on a table. Lock screen on laptop/tablet and close down after use. All confidential information must be safeguarded from access, no matter how unintentional, by anyone who has no need to know such as family and friends. This would be an unauthorised disclosure. Ensure that all confidential information is shredded when no longer required. Use strong security on a home WiFi connection.

20. Premises security

- Staff should be encouraged to challenge anyone in the clinic if they do not know who they are, e.g. if they are not accompanied by a member of staff or have an appointment with them.
- Staff should be aware of anyone they do not know attempting to follow them through a security door and if appropriate be prepared to escort them back to reception if necessary.
- Managers should ensure that all paper based records and any records held on computers are adequately protected. Risk assessments should identify any potential threats and an appropriate risk management strategy should be produced.

21. Online Safety

With the increase in virtual working the following are expected across all virtual platforms used by Growing Hope (e.g. zoom, facetime, whatsapp video, audio calling).

Zoom – Where zoom is used waiting rooms or individual password protected links should be used to help prevent meetings being hacked. Screen sharing should be set to 'host only' with the host only enabling participants to share when required. zoom links should never be posted in a public arena (e.g. on social media). Public events should always have a sign up option where a zoom link is then sent.

Adult supervision – Parent/ adult supervision is required for the majority of virtual sessions. Where counselling sessions are carried out in a 1:1 environment a parent should be present in the building.

Recording – In order to protect children and young people sessions can only be recorded or photographed with the written permission of all individuals involved. Therapists cannot record and send parents recordings of sessions, however, parents can record parts of

sessions to remember them if they would like to. Where written consent for photography has been given therapists can take photos of parts of virtual sessions to use for social media. Therapists should always verbally confirm this is okay with parents at the time of taking a photograph.

22. Data processing

The ways in which data is processed is outlined within the data mapping section below. This includes the processing of the following kinds of data:

- Emails
- Texts
- Post
- Photocopies
- Photos

This policy should be read alongside other Growing Hope policies.

Version: 4

Approved: **October 2020**

Amended: **March 2024**

Appendix 1 – Privacy notice

Growing Hope is committed to protecting the privacy and confidentiality of individuals who use our therapy services, our supporters and our staff and volunteers. This Privacy Notice outlines how we collect, use, disclose, and protect your personal information.

Types of Information Collected:

We may collect the following types of personal information:
For service users: Name, contact details, demographic information, health information, and any other information necessary to provide our services.

For supporters/donors: Name, contact details, payment information, donation history, and any other information provided voluntarily.

For staff and volunteers: Name, contact details, employment/volunteer history, qualifications, and any other information necessary for recruitment and management.

How Information is Collected:
We collect personal information through various channels, including:

- Service users: Referral forms, assessments, and interactions with our staff.
- Supporters/donors: Donation forms on our website, in-person donations, and communications with our fundraising team.
- Staff and volunteers: Job applications, resumes, interviews, and ongoing communications during employment or volunteering.

Purpose of Information Collection:
Personal information is collected for the following purposes:

- Providing services to children and families in need.
- Processing donations and gift aid forms.
- Managing staff and volunteer recruitment, training, and performance.
- Keeping supporters informed about our activities, events, and campaigns.

Legal Basis for Processing:
We process personal information based on:

- Legitimate interests will be used as the lawful basis to share the Personal Data of trustees, volunteers, freelancers and staff for the purpose of carrying out a business function. This includes in recruiting and interviewing for potential individuals to fill the roles above.

- Consent will be used as the lawful basis for sharing the Personal Data for children, young people and families accessing the Therapy Services. This consent will be given at the point of completing an online referral form.

- Legitimate interests will be used as the lawful basis for sharing the Personal Data of supporters of Growing Hope or local clinics

For Special Category Data:

- Employee health data: This is shared under the Article 6 lawful basis of legitimate interests for business purposes. The Article 9 condition for sharing this data is employment, social security and social protection law. This may include sickness records, maternity records, making reasonable adjustments for employees' work, and occupational health referrals. An appropriate policy document applies to the sharing of this data.

- Information about race, disability, gender and religious beliefs of employees, volunteers, trustees, service users or freelancers: This is shared under the Article 6 lawful basis of legitimate interests for business purposes. The Article 9 condition for sharing this data is Article 9(2)(d) not-for-profit bodies.

Data Sharing and Disclosure:
We may share personal information with third parties, including:

- Service providers assisting with program delivery and fundraising activities.
- Regulatory authorities to comply with legal obligations.
- Other organizations with consent or as required by law.

Data sharing between Growing Hope (national charity), the Local Growing Hope and the local Church who enter into a legal collaboration agreement when a local charity is set up:

Processing Activities

Growing Hope will:

- Share data with the Local Charity which enables the collaboration agreement to be carried out, such as, sharing referral personal data where Growing Hope have supported the collection of this data on the instruction of the Local Charity.

- Share data analysis with the Local Charity in order to support the process of fundraising.

- Share data with regards to general enquires, applications and interview tasks for employment, freelance engagement or volunteering.
- Share data with regards to supporters who have expressed interest in the Local Charity with the Local Charity.

The Local Charity will:

- Share Personal Data with Growing Hope for the purposes of families accessing training or support services.
- Share Personal Data with the Church for the purpose of supporting families to access Church activities.

The Church will:

- Share Personal Data with the Local Charity following general enquiries about the Therapy Services.
- Share information with the Local Charity for the purposes of working together, raising concerns and enabling the Therapy Services to run.
- Share information with the Growing Hope with regards to processes, policies and procedures necessary for building and facility use for this Agreement.

Data Retention:
We retain personal information for as long as necessary to fulfil the purposes outlined in this privacy notice or as required by law. Donation and service user records may be retained for financial reporting, auditing, and compliance purposes.

Security Measures:
We implement appropriate security measures to protect personal information from unauthorized access, disclosure, alteration, or destruction. These measures include encryption, access controls, and staff training on data protection.

Individual Rights:
Individuals have the following rights regarding their personal information:

- Right to access, rectify, erase, or restrict processing of personal information.
- Right to withdraw consent for processing personal information.
- Right to data portability (where applicable).

Contact Information:
For inquiries or concerns regarding privacy practices, please contact us at:
info@growinghope.org.uk

Changes to the Privacy Notice:
We may update this privacy notice periodically. Any material changes will be communicated through our website or other appropriate channels.

Consent:
By using our services, donating to Growing Hope, or providing personal information as staff or volunteers, individuals consent to the collection, use, and disclosure of their information as outlined in this privacy notice.

We do not knowingly collect personal information from children under the age of 13 without parental consent.

Jurisdiction-Specific Information:
This privacy notice applies to personal information collected by Growing Hope regardless of the individual's location.

Accessibility:
This privacy notice is easily accessible on our website and can be provided in alternative formats upon request.

Compliance Statements:
Growing Hope is committed to complying with relevant privacy laws and regulations, including the General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA).

Opt-Out Options:
We do not knowingly collect personal information from children under the age of 13 without parental consent.

Effective date:
1st March 2024

Appendix 2- Data Use

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Names, addresses, DOB, proof of ID for trustees	Controller - Growing Hope Local Charity. Support may be sought from Growing Hope to help process this data.	Legitimate interests for business purposes.	In order to complete application forms for banking, charity commission etc.	Within the Growing Hope GoogleDrive (in the HR folder- *only accessible by GH staff and CM for the relevant clinic)* Digital copies of personal ID will be saved within the Google Drive.	This data will be kept as long as the trustee is serving Growing Hope.	At the point that a trustee finishes their term their data will be deleted from the central list. This is the responsibility of the chair of trustees. Digital copies of personal ID will be saved within the Google Drive and deleted at the point a trustee finishes their term.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Copies of signed or completed forms by trustees	Controller- Trustees of the relevant Growing Hope charity.	Legitimate interests for business purposes.	In order that forms can be kept up to date and overviewed by the trustees of the local charity.	Within the Growing Hope GoogleDrive (in the local trustee folder- *only accessible by local trustees and national staff who are asked to support with processing this data. GoogleDrive account held by Growing Hope administrator account.*).	Data will be kept indefinitely as it forms a record of the process of the charity set up through which trustees can refer back to should they need to at a later date.	This data will be kept indefinitely as it provides a record of the charity set up and important documents completed. Paper copies of forms will be shredded once they have been approved and a digital copy will be kept within the Google Drive.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Names, addresses, contact information and professional information regarding employees	Controller – Clinic Manager/ Chair of trustees for Local Charity. Support may be sought from Growing Hope nationally to help process this data.	Legitimate interests for business purposes.	In order that the employee can be contacted if and when necessary outside of work. In order that payslips and any information related to employment can be sent.	Within the Canopy admin software system under the staff name. Within the local trustees Google Drive and personal drive of the Clinic Manager (sent as a password protected document from the Clinic Manager)	This data will be kept indefinitely as it forms a record of the employees of the charity	Data will be deleted from the personal account of the Clinic Manager if their employment is terminated. Accounts will then be suspended. If the new employee provides the information through a paper form or email this will be transferred into a password protected document which will then be sent to the trustees and stored within the Google Drive system. Any paper copies or the form or emails will be deleted.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
NI numbers, addresses and bank details of employees and freelancers for payment purposes.	Controller – relevant Growing Hope charity. Support provided by Growing Hope to help process this data for payroll and book keeping services.	Legitimate interests for business purposes.	In order that the individual who has completed work for Growing Hope can be paid.	Stored within a restricted section of the GoogleDrive for the and shared with the accounts team on a need to know basis. Any freelance invoices will be stored within this folder to keep a record of what has been spent.	This data will be kept indefinitely as it forms a record of the financial outgoings of the charity	Data will be deleted from the personal account of the Clinic Manager if their employment is terminated and will be transferred to the new Clinic manager. If the new employee provides the information through a paper form or email this will be transferred into a password protected document which will then be sent to the trustees and stored within the Google Drive system. Any paper copies or the form or emails will be deleted.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Contact details and information with regards to therapists who may potentially work for Growing Hope	Growing Hope (national charity) collects this data and shares it with relevant parties.	Legitimate interests for business purposes.	In order that the potential for new clinic set up can be tracked	This data will be stored within the relevant google drive accessed on a need to know basis.	In order that the progress and potential of new clinic set up can be tracked this will be kept indefinitely.	If an individual or church requests their removal from the Growing Hope system data will be deleted from the electronic file.
Referrals from potential families	Controller – the local clinic receiving the referrals. This data collection and processing is supported by Growing Hope nationally.	Consent – families consent to accessing support through the service.	In order so that potential referrals can be processed	This data is kept within password protected email accounts and is received via an online form completed on the growinghope.org.uk website. Referral forms are processed via JotForm (an encrypted system) and only shared with therapists working within the relevant local clinic. From time to time these may be accessed by the national charity to provide support to respond to queries.	In order that the journey of individuals accessing Growing Hope can be processed this information will be kept within the email systems.	If an individual requests their data is removed from the Growing Hope system their referral email will be deleted.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Letters received with regards to children being seen within clinic	Health professionals working within the local Growing Hope clinic		In order that a joined up approach between local professionals is encouraged and enabled by Growing Hope.	As soon as possible clinicians should scan or take a photo of these and then add them onto the Canopy system.	Clinical data will be kept as long as required, in line with health data requirements.	Once the letter is on the Canopy system the hard copy should be shredded. This letter will then be kept as long as required in its digital format.

Consent forms including informed consent and demographic data collection	Controller – Growing Hope local clinic. This data may be processed anonymously for monitoring and equality purposes.	Consent.	So that clinicians know that individuals have given informed consent for the use of their data and for their participation within the clinic setting. Demographic information is collated on this form in order that it can be completed at a time that is easy for the client. This information is then put into an anonymous database and used to inform	Consent forms are kept within the encrypted Canopy system which each individual clinician needs a password to login to. Demographic information is recorded by clinicians through input to a spreadsheet in the local clinic GoogleDrive.	Clinical data will be kept until as long as required in line with health data requirements. Demographic information will be collated and used anonymously indefinitely to inform impact statistics.	Once the form is on the Canopy system the hard copy should be shredded. This form will then be kept as long as required in its digital format. If the form is placed onto canopy through a photo being taken on a mobile phone this should be deleted as soon as possible.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Feedback forms including demographic data collection	Controller – Growing Hope local clinic. This data may be processed anonymously for monitoring and equality purposes.	Consent.	Feedback and demographic data is collated in order to provide impact and outcome information to members of the public and potential grant providers etc.	Data will be added onto a spreadsheet within the local clinic folder and shared with the trustees on request. Data will be kept anonymously and names will only be recorded and used where individuals have consented to this on their feedback form. Until the paper form is shredded it must be kept securely in a locked filing cabinet.	This data will be kept indefinitely in order to inform the impact reporting of Growing Hope.	Once the information on the form has been inputted electronically the paper form must be shredded. If individuals request that their quotes or feedback is not used by Growing Hope this will be deleted from the system.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Paper based assessments and notes taken within client sessions	Clinicians working within Growing Hope.	Consent	In order that assessments can take place and clinicians can record notes to inform their report writing.	Paper assessments should only be kept as long as necessary to write reports. This should be stored securely until the data is processed or destroyed. Where possible paper assessments should be completed with coded information (e.g. clients initials rather than full names) Clinicians should only transport this paperwork when necessary and should be vigilant with their bags. If the information is taken out of the clinic or office in order to work from home or be transported in between it should be shredded as soon as possible. This data should not be left in an unattended vehicle	The assessment reports informed by this information are to be kept indefinitely. Where information from these assessments may be needed in the future the clinician should upload a photo onto the canopy clinic software.	If assessment forms can be reused they should be completed in pencil and rubbed out as soon as possible. Where notes or forms are obsolete these should be shredded as soon as possible following the completion of the client report.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Clinical notes completed by freelance therapists	Clinicians working within Growing Hope	Consent.	In order that freelance therapists can work effectively and record clinical progress.	Personal notes should be stored securely at all times. By preference freelancers will have access to Canopy via a windows computer. If they do not have personal access to a windows computer they should send their notes password protected at the end of an intervention block of therapy to the Clinic Manager. These will then be directly uploaded to canopy.	Personal notes should be shredded at the end of a child's block of therapy. Notes which are uploaded onto canopy should be kept as long as required in line with health data requirements.	Personal notes should be shredded at the end of a child's block of therapy. Notes which are uploaded onto canopy should be kept as long as required in line with health data requirements.

Client reports, goal sheets, appointment letters and advice	Clinicians working within Growing Hope. Clients and professionals identified by clients.	Consent.	In order that clients can receive information about their therapy provision.	All reports, goal sheets, appointment letters and advice should be stored in a personal file on a clinicians password protected Growing Hope computer. Once these documents have been password protected (in the format Surname20XX) they should be uploaded to Canopy. Password protected reports and documents can be emailed to individuals outside of the organisation. Soft copies of documents should never be transferred without password protection. Where report data is for internal use it can be uploaded onto the Canopy system without a password. Clinicians working on a non Growing Hope device should only store data	Password protected files will be kept indefinitely as they inform the clients clinical record. Un-protected files should be deleted when the clinician ends their employment.	At the point of a clinician leaving Growing Hope their computer should be reset to factory settings before being passed onto another clinician. Reports and client related documents will be kept in a password protected format or securely within the Canopy system indefinitely.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
				in the 'my drive' section of their GH GoogleDrive folder.		
Client contact numbers and emails used for reminders/ communication	Clinicians and administrators specific to families they are working with	Consent.	To be able to communicate with clients and keep them up to date with what is happening.	Contacts will be stored within the Growing Hope email system or on a Growing Hope phone. If a clinician needs to make a call from a personal phone they should withhold caller ID. If they need to send a text reminder they should do this in collaboration with the and Clinic Manager from the clinic phone. At no point whilst the child is being seen in clinic should personal numbers be used or exchanged. Should clients become involved members of the church community then personal numbers may be exchanged at an individual's discretion in the capacity of a friend not health care professional.	Data will be kept whilst working with the client.	Emails will remain on the local clinic system in order that families can remain informed about clinic events. If families ask for their numbers or email contact to be taken off the list these will be deleted. Contacts stored in phones will remain there but will be wiped if the clinician leaves the practice.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Supporter bank details from paper giving forms	Controller – Growing Hope local clinic. This data may be processed anonymously for monitoring and equality purposes.	Legitimate interest.	To be able to input bank details into the online direct debit system and keep a record of who is giving	This data will be kept in a folder in the 'my drive' section of the finance trustees Growing Hope login. This will only be shared with the finance volunteer if they input this data in. Until the data can be recorded on the spreadsheet paper based forms will be kept in a locked filing cabinet.	One master spreadsheet which is password protected will be kept indefinitely in order to make sure that donors can be tracked and thanked where appropriate. Spreadsheets used for uploading data into the CAF regular giving system will be deleted following upload.	Paper giving forms will be shredded as soon as they have been inputted into the spreadsheet.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Supporter data via online giving (e.g. JustGiving, CAF etc)	Growing Hope charity.	Consent and legitimate interests.	To be able to track and monitor regular givers	This data will be kept safe within the GDPR policies of the organisation who is managing the data. Individuals will be giving consent by choosing to process their donation through another agency. Where individuals consent to passing on their data to Growing Hope this will be inputted into an existing data system (e.g. mail chimp for mailing list). As part of the security protocols when using the CRM tools used to support Growing Hope's daily work (including Sales Force, Quickbooks, Mail Chimp and other data collection avenues) Growing Hope National staff can access the entire database, however local clinic managers and staff can only access data in relation to their own individual clinics.	Data will be kept indefinitely within the systems and will be deleted inline with the policy of the system the supporter has signed up via.	Data will be kept indefinitely within the systems and will be deleted inline with the policy of the system the supporter has signed up via.

Supporter data via bank statement- names and records of giving	Controller- Growing Hope charity Processing may be supported by Growing Hope nationally as part of payroll and book keeping services.	Legitimate interest.	In order that the finance trustee can manage the finances of the organisation they have access to the bank account. In order that the Clinic Manager can make purchases in line with the budget agreed using a Growing Hope card.	Login to the bank system is only given to individuals as agreed when the bank account is initially set up. All data is held securely within the banking system in line with the bank's data protection policy. Downloaded statements used for processing finances will be kept within the 'my drive' section of the finance trustees Growing Hope login. These should only be used for budgeting and processing purposes. The bank account is directly linked to the Quickbooks system which helps with annual reporting of accounts and processing and managing receipts. It is the responsibility of the finance trustee together with the finance volunteer to keep this up to date. Annual reports of the charities finances will not contain any personal data of who has given and how much.	Banking information is kept indefinitely in order to keep a record of the charity's financial position.	Should the bank account be closed or transferred one electronic password protected copy will be kept by the charity trustees in order to be able to review finances. If the finance trustee changes their Growing Hope account will be deleted and files transferred to the new finance trustee. The new trustee will be able to access statements via the bank account. Budget documents not directly related to actual spends are kept within the trustee folder.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
List of names of supporters giving regularly and giving one off	Relevant Growing Hope charity.	Legitimate interests.	In order that trustees and the fundraising committee are aware of who is giving regularly in order that they can be thanked for their support and updated with regards to the charities progress.	This list will be kept in a password protected document only accessible by the local trustees and fundraising committee. The document will only contain names (no amounts or other details).	This document will be kept up to date with individuals currently giving.	If individuals stop giving regularly their name will move to the one off giver list. If individuals request their data is removed from the Growing Hope system their name will be deleted from the list.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Growing Hope financial information including budget summaries	Controller – relevant Growing Hope charity. This process may be supported by Growing Hope national finance team where requestsed.	Legitimate interests.	In order that everyone is aware of the budget and the plan for spending in order that this can be managed well and that where there is deficit every effort can be made to rectify this.	The budget will be kept within the trustees folder and circulated at trustees and fundraising committee meetings as and when necessary. Paper copies of the budgets will be kept securely and disposed of by shredding when they have been used.	This will be updated regularly and kept indefinitely in order to track the budget and expenses.	This will be updated regularly and kept indefinitely in order to track the budget and expenses.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Login details for general use accounts e.g. solopress, CAF, Just giving, Charity commission.	Relevant Growing Hope charity.	Not personal data.	In order that access to accounts is possible and can happen efficiently.	The password document will be password protected with a password known only to the trustees and Growing Hope National staff. This will enable access to the information when required. Where information is sensitive and should not be shared (e.g. bank login) trustees will keep their own password document within the 'my drive' section of their growing hope account.	Indefinitely in order that accounts can be accessed. This would be deleted if the charity ceases to exist.	Information will be updated and deleted electronically as and when necessary.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Gift aid forms and gift aid spreadsheets	Controller- Relevant Growing Hope charity. Growing Hope national charity may help with processing this with consent.	Consent.	In order that gift aid can be processed and managed.	The online gift aid form will be completed by individuals and sent to the accounts@growinghope.org.uk email address. This will then be forwarded onto the relevant local finance trustee. Gift Aid forms will be kept in a folder in the 'My Drive' of the finance trustee which will only be shared with the finance volunteer. Gift aid emails (generated from individuals inputting their information through the website) and photos of paper based gift aid forms will be uploaded into this folder. Spreadsheets of the gift aid forms uploaded onto the government website will be stored within this folder.	Indefinitely in order that we can track the finances and gift aid.	N/A

Growing Hope supporter database	This data is controlled and processed by the relevant Growing Hope charity. Growing Hope nationally support with processing this data for marketing purposes.	Consent.	In order that we have a national database we can send newsletter information and communications to.	This is collated through opt-in at www.growinghope.org.uk/get-involved When individuals sign up by paper forms, the information will be uploaded electronically and shredded. The data is stored on mailchimp and salesforce and then used by the trustees / GH staff to send out mailings As part of the security protocols when using the CRM tools used to support Growing Hope's daily work (including Sales Force, Quickbooks, Mail Chimp and other data collection avenues) Growing Hope National staff can access the entire database, however local clinic managers and staff can only access data in relation to their own individual clinics.	This data will be kept indefinitely but supporters can opt out of data storage or receiving information from Growing Hope.	Individuals are able to unsubscribe themselves in order to opt out of receiving communications from Growing Hope. Paper based sign ups will be shredded as soon as they have been added to the online system.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Other data relevant to Growing Hope clinics (without any personal data)	The relevant Growing Hope charity	Not applicable.	The trustee folders for each clinic will contain information about running the charity. The clinic folder for each clinic will include the master file for the canopy software and any information relevant to the clinic.	Every individual will have a Growing Hope login to GoogleDrive. Trustees will have access to the Growing Hope *local* Trustee file (also accessible by the National trustees). Clinicians will have access to the Growing Hope *local* Clinic file (which will contain the encrypted directory to Canopy client data). Individuals can keep personal files in relation to the charity in the 'my drive' section of their GoogleDrive or saved within the harddrive of a Growing Hope computer which is password protected. Employees should be vigilant when transporting their laptops and make sure that these are kept securely and not left unattended in vehicles.	Ongoing (non-personal)	Deleted from drive when no longer relevant

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Shared email accounts (e.g. info@ accounts@ *local*@ email addresses)	Relevant trustees or administrators	Legitimate interest.	In order that queries specific to an area of the charity or a whole team can be picked up more quickly and efficiently and information can be shared more readily.	The password of each general email account is only to be shared on a need to know basis. Any personal data will be sent in a password protected document.	Personal communications via email will be stored within the email system in order that these can be tracked if there is a query.	Archived as prompted by the email system.

Type of data	Who is the controller/ processor?	What is the lawful basis of processing?	What is the purpose of this access?	How is this data kept safe?	How long will we keep this data?	How and when is this data destroyed?
Post received into clinic and posted out	and Clinic Manager or appropriate clinician	Legitimate interest.	To share information directly with other organisations in relation to a child's care.	Letters received by a clinician will be scanned and added to canopy and then shredded at the earliest opportunity. Until then they are to be stored securely. Letters posted should be printed only on a needs basis and should be shredded if they are not sent. They should be posted within 24hrs of printing. Where reports or sensitive data are printed for giving to families within clinics these should be stored securely until this has taken place.	Personal data will all be stored on canopy indefinitely in order to protect each child's health care data.	Paper copies of letters and reports will be shredded as soon as they are uploaded into canopy.

Photographs and videos of individuals within clinic	The local charity.	Explicit consent.	In order that when consent is given by parents and children, we can use these photos and videos to promote Growing Hope. Promotion may be through Twitter, Instagram, Facebook, flyers, the website, newsletter, presentations and other channels.	Photos and videos should only be taken when there is written informed consent on the consent form completed at the time of the assessment and with informed verbal consent at the time of taking the photo or video. Whatsapp (which encrypts data) will be used to pass on photos and stories to the Social media officer and newsletter writing trustee in order that these can be added in to the Growing Hope story and used as appropriate. As families have given consent for these to be shared those going on social media can remain on the clinic phone. If a clinician is using a personal not Growing Hope phone photos and videos should be sent on and deleted immediately.	Data will be kept indefinitely on social media channels. Photos which have informed consent will be sent internally through a Growing Hope email address in order that they can be saved within the national trustees team drive and used for design. These photos can also be stored within the design files of the local trustees.	Photos and videos will be kept indefinitely on social media and within GoogleDrive folders in order that the story of clinics can be tracked across the years.

Growing HOPE

Providing free therapy for children and young people with additional needs and their families in partnership with local churches across the UK.

Further information about Data systems and storage within Growing Hope

Canopy

Canopy is the clinic software system which is used to store the majority of personal data which is processed by Growing Hope (https://canopyadminsoftware.com/). This is an encrypted clinic software in which health professionals can login, input and store data such as client names, carer names, DOB, contact details and clinical notes. The software also stores contact details of other relevant professionals and staff information. The software is used for timetabling and room booking management and this can be configured by the local clinic. Each local clinic will have a master file used for canopy so client data cannot be accessed between local Growing Hope clinics. Canopy encrypts client data so that it cannot be accessed by individuals who do not have a login.

Email Accounts

All Growing Hope volunteers, employees and trustees will be set up with a personal Growing Hope email account (firstname.surname@growinghope.org.uk) at the point of starting their employment with Growing Hope if they require access to the Growing Hope file system. Their email account will be set up by Growing Hope National charity and the individual will be required to personalise their password upon setting up the account. This account will then be added to the appropriate *Team Drive* within the GoogleDrive system.

At no point should personal emails or personal online file systems be used for Growing Hope purposes.

General email addresses such as accountslocalclincname@growinghope.org.uk or localclinicname@growinghope.org.uk will be set up when the clinic launches and access will only be given on a needs basis (for example to finance trustee and finance volunteer, administrator and clinic manager).

GoogleDrive

GoogleDrive is used by Growing Hope in order that all organisational files are kept securely in one system. The GoogleDrive is managed centrally by the Growing Hope trustees and is divided into *Team Drives*. Each Growing Hope local will have one team drive for their

general data and files **Growing Hope *local name* Trustees** (only accessed by trustees) and one team drive for their canopy software system client and clinic files **Growing Hope *local name* Clinic** (only accessed by employees and freelancers working with families). In addition to this there is a clinic set up team drive which can be shared within individuals outside of the organisation considering setting up a Growing Hope (this folder does not contain any personal data). We are confident that in line with GDPR guidelines GoogleDrive have done what they can to ensure that files and folders can only be accessed by those granted access within the drive system- this means that each individual working with Growing Hope will have a password protected account which will enable them to access the files appropriate to them.

Trustees may access GoogleDrive through 'Google file stream' which will download files onto their computer. Trustees should therefore make sure that they have a secure login for their computer which is not shared with other individuals.

Laptop policy

Personal data and general information may be stored on Growing Hope laptops which are password protected. Information should not be transferred between laptops or accessed via online storage (other than GoogleDrive) unless absolutely necessary- if this is the case all documents should be password protected or stored on an encrypted device.

The 'my drive section' should be used for personal Growing Hope files and if files need to be shared with a small number of individuals (rather than all clinicians or all trustees) they should be placed here and specifically shared.

Data-stick policy

Any USB sticks used for personal data must be encrypted.

Mobile phone policy

All clinicians employed by Growing Hope more than 2 days a week will receive a phone that they can use for Growing Hope purposes.

If individuals without a Growing Hope phone are using their personal phone within the clinic setting the following guidelines apply. Any photos taken for social media or in order to scan in and process documents must be uploaded to Canopy or sent onto the social media team and deleted within 24hrs of being taken. The phone used must be password protected and only used by the individual.

GDPR Training

All Growing Hope employees should undertake an online module to train them in GDPR processes and procedures. All employees, volunteers and trustees should have fully read this policy and signed a non-disclosure agreement.

Social Media Policy

Social media posts are to be made by the social media officer contracted through Growing Hope National. Communication and sharing of information to post will be done through the structures outlined above. Where possible photos and videos used for this social media should only be taken on a Growing Hope phone by a Growing Hope employee. Photos and videos should only ever be taken and used where written and informed consent has been given and expressed consent has also been given at the time of capturing the photo/video.

Under no circumstances are photos of children, young people and adults, names or personal details to be disclosed on a clinician, trustee or volunteer's personal social media profile. Social media posts made by Growing Hope (@growinghopeuk) in line with the consent process above can be shared by employees, volunteers and trustees. At public events individuals can use their personal social media to post general photos and videos that do not focus on a certain individual unless they are doing so on the basis of a friend relationship with informed consent.

Photography and videos can be taken of a child, young person or adult for communication purposes with their parents with the child, young person or adult's own phone or ipad (with expressed request

and consent from the parent/carer).

Volunteers/Trustees/Clinicians are able to be in photos requested by individuals and their families if the volunteer/trustee/clinician consents to this.

Data breaches

Where a breach of personal data occurs this should be reported to the trustees of the charity and the data protection officer (national charity) as soon as the breach is realised. Where the breach presents a high risk to individuals through adversely affecting their rights and freedoms they should be notified and the breach must be reported to the ICO within 72hrs. The most appropriate person to report this will be decided with the input of the data protection officer and local charity trustees.

Where a breach is discussed by trustees and the data protection officer and is felt not to be of high risk to individuals then it should be recorded within the 'data breaches' folder of the trustees GoogleDrive. This ensures that a record is kept of what has happened and the action taken with regards to the breach. This should be monitored and returned to if any issues arise as a result of the breach.