	Title	**Information Governance Policy**
	Version	Version 3
	Date	03.09.19
	File Reference	• Hillingdon4All - Documents\IG • Wellbeing Team Site - Documents\Information Governance\Policies

Summary	This document details the H4All CIO policy for Information Governance
Next Review Date	18.07.2020
Policy Lead	Dalvinder Jammu
Persons Covered	Board of Directors, Chief Officers, Staff, Volunteers, Secondees, People on Placement, Clients, Donors, Contractors and other relevant Stakeholders

Change History	Version	Date	Main Changes	Changed By
	2	04.03.2019	• Charity number amended • Inclusion of Location/Geotag data • Addition of Legal Basis for processing • Removal of named CRMs	Dalvinder Jammu
	3	03.09.19	• Addition of H4All CIO following conversion to charity • Addition of Accessing Personal Records	Dalvinder Jammu

Approvals	Author	Name	Signature
	Service Manager	Dalvinder Jammu	*D. Jammu*
	Authorised	**Name**	**Signature**
	Chief Executive	Angela Wegener	*A. Wegener*

Related Documents

- Privacy Notice
- Privacy Impact Assessment
- IG Training Guidance document
- Procedure for the secure transfer and receipt of personal and sensitive information
- Data Breach Procedure
- Grievance Policy
- Whistleblowing Policy
- Disciplinary Policy

Please do not cite without the prior permission of H4All CIO
Any amendments are detailed on the Policy Information / Amendment Tracking Form at the end of the Document

Contents page

1. Introduction

Information (data) is a vital asset, both in terms of providing information on/for client's, staff, volunteers, trustees, donors, contractors, suppliers and other relevant stakeholders and for providing information to ensure the efficient management, development and delivery of services and resources.

It is therefore of paramount importance that information is efficiently managed and that appropriate policies, procedures, management accountability and structures are in place to provide a robust governance framework for the management of information.

H4All CIO fully supports the principles of Information Governance and recognises the role it plays in the security arrangements to safeguard stakeholder data. H4All CIO holds data on the people who use its services, the people involved in providing the service, the people who support the aims of the organisation, professionals and contacts in other organisations and suppliers/contractors. The most important way in which H4All CIO use data is in providing clients with services to improve health and wellbeing and to support them to live independently.

This policy sets out H4All CIO's undertaking to keep information up to date and accurate and to do everything we can to prevent it from being used in any unauthorised or unlawful way. It also sets out the systems and processes used to ensure that the organisation complies with current legislation and best practice.

This policy applies to all personal data processed by H4All CIO and complies with the principles of the General Data Protection Regulations (GDPR). The GDPR came into force on the 25 May 2018 and defines the rights of an individual in relation to the information held about them and how it is captured, stored, used and shared.

It should be read in conjunction with our Privacy Notice, Privacy Impact Assessment, IG Training Guidance document, Procedure for the secure transfer and receipt of personal and sensitive information, Data Breach Procedure, Grievance Policy, Whistleblowing policy and Disciplinary Policy.

Failure to adhere to the rules and policies set by H4All CIO will be regarded as gross misconduct and likely to result in disciplinary action in accordance with other policies of H4All CIO.

1(a). Definitions

Data Subject – used to denote an individual (or organisation) about whom data is processed.

Data Controller – used to denote the entity with overall responsibility for data collection and management who must ensure that data is processed according to the law and data processing principles.
H4All CIO is the Data Controller.

Data Processor – a person or organisation who processes data on behalf of and on the orders of a controller.
H4All CIO is the Data Processor.

Processing of Information – the terms 'process', 'processed' or 'processing' apply to any activity involving data, such as 'collecting', 'storing', 'sharing', 'removing' or 'destroying'.

Personal data – is any information related to a natural person, that can be used to directly or indirectly identify the person.

Special Category Data - is personal information that is considered more sensitive and needs more protection under the GDPR and requires the individual's explicit consent for it to be processed.

Data Breach – a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data and/or a security incident that has affected the confidentiality, integrity or availability of personal data.

Lawful Basis - The lawful basis for processing data are set out in Article 6 of the GDPR. At least one of these bases must apply whenever personal data is processed. H4All CIO must have a valid lawful basis in order to process personal data – before the data is processed. This cannot be changed later.

Privacy Notice – is a key document which organisations must have if they collect, use or process personal data of European Union citizens. This document informs what is done with the personal information of individuals.

Information Commissioners Office (ICO) - The UK's independent authority, set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Supervisory Authority (SA) - In regard to GDPR, each country will have its own supervisory authority; for the UK the Information Commissioner's Office is the Supervisory Authority.

Data Protection Officer (DPO) - is a leadership role required by the GDPR. Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

Subject Access Request - gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

1(b). Scope

This policy applies to H4All CIO, the registered charity, its sovereign partners and its subsidiary companies.

1(c). Purpose of the policy

This Information Governance (IG) policy provides an overview of H4All CIO's approach to IG; a guide to the procedures in use and details about the IG management structures within the organisation. This policy should be read in conjunction with H4All CIO Privacy Notice, Privacy Impact Assessment, IG Training Guidance document, Procedure for the secure transfer and receipt of personal and sensitive information, Data Breach Procedure, Grievance Policy, Whistleblowing policy and Disciplinary Policy.

1(d). Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR) 2018
- The Data Protection Bill 2017
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection Regulations 2004
- The Equality Act 2010

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of GDPR'
- Information Commissioner's Office (2017) 'Preparing for the GDPR 12 steps to take now'

1(e). Legal Compliance

- H4All CIO will implement and maintain policies to ensure compliance with current and relevant Data Protection regulations/principles, Confidentiality principles and the Human Rights Act
- H4All CIO will implement and maintain policies and procedures for;
  - the controlled and appropriate processing of information, in particular in relation to the safeguarding of vulnerable adults and children
  - the effective and secure management of its information assets and resources
  - information quality assurance
  - the effective management of records and data
- H4All CIO will promote effective confidentiality, data and record management and security practice to its personnel, through policies, procedures and training
- The legal basis for sharing information will be made clear to the data subject at the time the information is processed
- Individuals will be provided with information on what data is held on them and how it will be processed
- Individuals will be made aware that they have a right to make a Subject Access Request, how to do this and the 30-day response time limit
- H4All CIO will have clear procedures and arrangements for dealing with complaints
- H4All CIO will have documented procedures on disciplinary action, making reference to non-compliance against IG procedures and a documented grievance procedure
- H4All CIO will implement and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and/or information security and take corrective action as required
- H4All CIO will take ownership of, and seek to improve, the quality of information within its services and wherever possible, information quality will be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards
- H4All CIO will seek individuals' consent before using any personal or sensitive information or images in any marketing/publicity materials

1(f). Accountability

H4All CIO will implement appropriate technical and organisational measures to ensure that data is processed in line with the principles set out in the GDPR.

H4All CIO will provide a comprehensive, clear and transparent Privacy Notice.

Additional internal records of H4All CIO's processing activities will be maintained and kept up-to-date.

H4All CIO undertakes to implement IG effectively and will ensure the following:

- Information will be protected against unauthorised access/loss/damage/theft
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Regulatory and legislative requirements will be met
- Business continuity plans are produced, maintained and tested
- IG training guidance will be given to all relevant staff, volunteers, secondee's and relevant stakeholders, as appropriate to their role
- All breaches of confidentiality and information security, actual or suspected, will be logged and/or reported and investigated
- H4All CIO will meet our obligations for reporting to the ICO when required and within the 72-hour deadline

1(g). Responsibilities

The designated lead for IG is Dalvinder Jammu, Service Manager for H4All CIO. The operational lead for Information Governance is Angela Wegener Chief Executive for H4All CIO.
The senior managers are responsible for ensuring appropriate systems and processes are in place within their areas of responsibility.
All personnel are responsible for ensuring that they are aware of and comply with, the requirements of this policy and the procedures and guidelines produced to support it.

2: Lawful Basis for Processing Data

All data processed by H4All CIO must be done under one of the following 'Lawful Basis'; **Consent, Contract, Legal obligation, Vital interests, Public task or Legitimate interests** (see ICO guidance for more information).
Article 5 of the GDPR requires that personal data be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. Accurate and kept up to date

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
   See Appendix A: H4All CIO Data Retention Schedule November 2018
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
7. Not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates

2(a). Consent

H4All CIO uses **Consent** as its main lawful basis for processing data for clients. This means that H4All CIO need data subject explicit consent before H4All CIO can process data. The types of data we may process includes, but is not limited to:

Client Data	
H4All CIO collect the following personal data:	H4All CIO collect the following special category data:
• Name • Address • Contact Information/Emergency Contact Information • NHS Number • GP Surgery / GP Name • Professional(s) involved in care • Online identifiers such as an IP address	• Gender • Date of Birth/Age Range • Marital status • Race / Ethnicity • Religious Group • Main Language spoken • Health • Disability • Living Arrangement/Accommodation Type • Genetic/Biometric
Employee/Volunteer Data	
H4All CIO collect the following personal data:	H4All CIO collect the following special category data:
• Name • Telephone number/Emergency contact details • Home/Business address • Bank Account/Financial details/Tax code • Passport/Driver license/NI number • Photographs • Employment terms and conditions • Employment History with the organisation • Start date/Leaving date and the reason for leaving	• Gender • Sexual history/Orientation • Marital status • Race/Ethnicity • Religious Group • Main Language spoken • Health/Medical/Injury • Disability • Living Arrangement/Accommodation Type • Genetic/Biometric • Location/Geotag

• Training records and professional memberships • Compensation history • Disciplinary and Grievance records • Absence records (sick/holiday leave) • Any work-related accidents/injuries • Education and qualifications • Recruitment information • Work experience • Results of HMRC employment status check • Performance information • IP address • CCTV footage and other information obtained through electronic means such as swipe card records • Information about the use of our information and communications systems	• Political membership or opinions • Trade union membership • Criminal Records

Consent must be; freely given, specific, informed, unambiguous, not a precondition of using the service and separate from other terms and conditions. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent must be a clear affirmative action which signifies agreement to H4All CIO to process data such as by a written statement, an oral statement or electronic means (this could include actively ticking a box when visiting an internet website or choosing technical settings) or any other statement or conduct which clearly indicates in this context data subject acceptance of the proposed processing of data.

Where consent is given, a record will be kept documenting how and when consent was given.

Consent will cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent must be given for all of the purposes individually. Any third parties with whom the data may be shared with will be specifically named and H4All CIO will inform of:

- where each individual referral will be made to
- what data will be shared
- how the data will be shared

Where data is not obtained directly from the data subject, information regarding the categories of personal data that H4All CIO holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

2(b). Consent to share Data

Data subject individual consent to share information should always be checked before disclosing personal information to another agency.

It is an offence to disclose personal information 'knowingly and recklessly' to third parties.

If H4All CIO have data subject consent H4All CIO may share data with partners who, with H4All CIO, are jointly delivering an activity or service. This could include sharing data with a third-party organisation who are a network partner, provide a service to/for H4All CIO, work with/for H4All CIO in the delivery of services, act as data processors for H4All CIO, act as fundraisers for H4All CIO or provide HR/payroll information, marketing and communication services for H4All CIO.
H4All CIO will undertake due diligence on these third parties and will require them to comply strictly with data protection policies and legislation.

H4All CIO may also share data in the following circumstances:

- Where H4All CIO must comply with laws such as those for national security, taxation, or criminal investigations.
- Where H4All CIO must undertake due diligence, to be sure we are not being used as a channel for criminal activities.

H4All CIO will not share your data with other organisations for any other purposes.

H4All CIO will ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease.

Consent accepted under the Data Protection Act 1988 (DPA) will be reviewed to ensure it meets the standards of the GDPR. Where the consent obtained under the DPA is acceptable, H4All CIO are not required to reobtain new consent for historic records.

2(c). Consent not given

The data subject can choose not to give consent to H4All CIO to process data. In this instance the data subject will still be able to receive a limited service from H4All CIO, but no identifiable record will be kept of their interactions with H4All CIO.

The data subject can choose to withdraw previously given consent to H4All CIO by contacting H4All CIO directly in writing. When this has been requested, the information in question will be removed from H4All CIO secure system(s) and the data subject will be informed in writing. No identifiable record will be kept of their interactions with H4All CIO.

In both of these instances data subjects would have limited ongoing recourse as no identifiable record will be kept of their interactions with H4All CIO.

2 (d). Additional Legal Basis

Although H4All CIO uses consent as its main lawful basis for processing data, H4All CIO will also utilise the following legal basis's when appropriate or required by law:

1. **Contract**: when the processing of data is necessary for a contract H4All CIO have with the data subject, or because a data subject has asked H4All CIO to take specific steps before entering into a contract.

2. **Legal obligation**: when the processing is necessary for H4All CIO to comply with the law (not including contractual obligations), for example supplying HMRC with mandatory employee data.
3. **Vital interests:** when the processing is necessary to protect someone's life.
4. **Legitimate interests**: when the processing is necessary for H4All CIO's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

3: Data Protection

H4All CIO is committed to processing data in accordance with its responsibilities under the GDPR.

H4All CIO holds data on the people who use its services, the people involved in providing the service, the people who support the aims of the organisation and professionals and contacts in other organisations. The most important way in which H4All CIO use data is in providing clients with services to improve health and wellbeing and support them to live independently.

3(a). Data Security

H4All CIO have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

In the main data is stored on secure electronic cloud-based Customer Relationship Management (CRM) systems e.g. Charitylog or secure electronic a cloud-based document management and storage system, e.g. SharePoint.

When commissioning cloud-based systems, H4All CIO will satisfy themselves as to the compliance of data protection principles and robustness of the cloud-based providers.

All necessary members of staff, secondee's, volunteers and Trustees are provided with their own secure login and password, and every IT system regularly prompts users to change their password.

Staff may not use personal (i.e. not supplied by H4All CIO) IT systems for H4All CIO purposes, including accessing H4All CIO/NHS email accounts, CRM systems and downloading documents.

All necessary Trustees and/or Members will be given access to relevant H4All CIO documents via secure remote access; these documents must be downloaded or printed only as necessary; any hard copies of these documents must be brought to the relevant H4All CIO offices for secure disposal once no longer required. Electronic copies must be securely deleted from any private IT systems including any metadata relating to the document. Emails containing personal data will be deleted once no longer required for the initial purpose.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of H4All CIO containing sensitive information are supervised at all times.

The physical security of H4All CIO's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

3(b). Electronic/Digital Records

With consent client data is stored on secure electronic, cloud-based, CRM system(s); or a cloud-based document management and storage system(s).

Staff, secondee, volunteer and organisational data is stored on a secure electronic, cloud-based, CRM system(s); or cloud-based document management and storage system(s).

Data should only be stored on the server or cloud-based systems and not on individual computers.

Digital data is coded, encrypted or password-protected, on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be password-protected and kept in an appropriate lockable cupboard or cabinet when not in use.

Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipient; or the data shared is suitably pseudonymised with a unique ID number used to identify the client.

When sending confidential information, staff will always check that the recipient is correct before sending.

Before sharing data, all staff members will ensure:
- they are allowed to share it
- that adequate security is in place to protect it
- that whoever the data is being shared with has been clearly outlined

Circular emails are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

Where electronic records are taken off the premises, staff will take extra care to follow the same procedures for security.

The person taking the information from the premises accepts full responsibility for the security of the data.

When working off-site, all data protection and confidentiality principles still apply.

Data is never left unattended and/or in clear view during the working the day.

3(c). Paper Records

Confidential paper records are kept in an appropriate lockable cupboard or cabinet when not in use, with restricted access.

Workstations operate a clear desk policy so that any confidential paper records are not left unattended or in clear view anywhere with general access.

Where confidential paper records are taken off the premises, staff will take extra care to follow the same procedures for security and ensure that lockable crates are used to secure paper records in transit.

The person taking the information from the premises accepts full responsibility for the security of the data.

Any paper records that are no longer required (including 'scrap paper' that contains personal data) must be shredded and disposed of appropriately.

When working off-site, all data protection and confidentiality principles still apply.

Data is never left unattended and/or in clear view during the working the day.

4: Data Breaches

The term 'data and/or information breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data and/or a security incident that has affected the confidentiality, integrity or availability of personal data. This includes breaches that are the result of both accidental and deliberate causes.

H4All CIO will ensure that all staff members are made aware of, and understand, what constitutes a data breach.

4 (a) Breach notification

Effective and robust breach detection, investigation and internal reporting procedures are in place at H4All CIO, which facilitate decision-making in relation to whether the ICO or the public need to be notified.

Within a breach notification, the following information must be outlined:

- the nature of the data breach, including the categories, type of data and approximate number of individuals and records concerned
- an explanation of the likely cause of the data breach
- an explanation of the likely consequences of the data breach
- a description of the proposed measures to be taken to deal with the personal data breach
- where appropriate, a description of the measures taken to mitigate any possible adverse effects
- the name and contact details of the DPO

Where a breach is likely to result in material or non-material harm; or risk to the rights and freedoms of individuals, the ICO will be informed within 72 hours of H4All CIO becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis by the DPO.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, H4All CIO will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO.

In the event that the DPO has deemed an information breach sufficiently serious to notify the ICO then consideration must be given to also notifying the Charity Commission. The DPO and/or lead Chief Executive will discuss the situation with the Board of Directors and agree if a report needs to be submitted. The Charity Commissions "Reporting Serious Incidents – A Guide for Trustees" document should be referred to and the process defined by the Charity Commission followed.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

If the decision is made that the breach does not need to be reported, then the DPO will need to be able to justify this decision and document this accordingly.

H4All CIO takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The DPO is responsible for ensuring that continuity and recovery measures are in place to ensure the security of protected data.

This policy should be read in conjunction with H4All CIO Breach Procedure November 2018.

5: IT Systems

In this instance the term IT systems is used to denote any fixed and portable computers, laptops, smartphones, tablets or any other device capable of accessing the internet or email, IT systems via remote access, software, licences, dedicated website(s), email and Customer Relationship Management (CRM) systems e.g. Charitylog that are provided for the purposes of H4All CIO and belong to or are licensed/made available to the organisation.

H4All CIO's commitment to ensuring data protection and confidentiality requires us to ensure that our IT systems and peripherals are secure, used and maintained appropriately by all staff.

H4All CIO reserves the right to monitor usage of its IT systems and facilities, including, but not limited to, auditing programmes, analysing the contents of data files and storage areas, reviewing deleted and accessed data, access to folders/documents, monitoring email usage, monitoring websites accessed and recent searches/browser history. This applies to IT systems used on or H4All CIO sites and for H4All CIO business.

IT systems should be used only by H4All CIO workers or by people authorised by H4All CIO; explicitly for H4All CIO purposes.

Each individual is responsible for the security of IT systems used and must not allow it to be used by an unauthorised person or in an unauthorised way.

5 (a). Use of IT Systems

IT systems should not be used to send email or access the internet (including social networking sites) for non-business purposes. This applies whether during working hours or non-working hours. If any IT systems are used to access systems such as email or the Internet for private use, such usage may be monitored and recorded. Use of these systems for the purpose for which they are not intended may result in disciplinary action and may constitute a criminal offence.

Internet and email usage must always accord with H4All CIO policies and procedures. Infringements may result in disciplinary action. Below are typical of infringements H4All CIO regard as serious. The examples below are indicative and not intended to be exhaustive:

- Sending messages or images that are potentially offensive, libellous, obscene or contravene our equal opportunities policy or organisational ethos
- Sending messages or images that could constitute bullying or harassment or are potentially detrimental to the organisation's interests
- Accessing, downloading or distributing pornographic images, graphics or text depicting nudity, intercourse or sexual acts, obscene or indecent material from any source is forbidden and may be grounds for immediate dismissal. The storing and transfer of such images using H4All CIO IT systems is forbidden
- Playing games, gambling, use of chat lines, watching TV channels
- Excessive or inappropriate use of mailing lists, etc. is not allowed using H4All CIO IT systems
- Downloading or distributing copyright information and/or software without express approval
- Setting up websites, web pages, blogs etc. using H4All CIO IT systems or in our name without express approval
- Publishing images, pages or contributions on external websites (including social networking sites) without express approval. This restriction relates to our organisation, any employee, client, supplier, stakeholder etc.
- Buying or selling things and engaging in online auctions on your own behalf or in our name without express approval
- Buying goods via a credit card transaction for business use should only be done with the approval of the Chief Executive.

Use of email and the internet (including social networking sites) must accord with all legal obligations and have specific regard to the following:

- not use personal email or social networking accounts to conduct official H4All CIO business
- not post defamatory or derogatory statements about H4All CIO, our employees, clients, suppliers, stakeholders etc. This applies to business and personal email. It also applies to all contributions made on internet/social networking sites.
- not upload, download or otherwise transmit commercial software or any other copyright materials belonging to others. Express authorisation must be received before doing so even where H4All CIO is licensed to use such material.

An offence is committed under the Computers Misuse Act and/or the GDPR if you:

- use IT systems for any illegal purposes
- access programs or data with the intent to commit or facilitate the commission of an offence
- intentionally make unauthorised modification of computer programs or data held in a computer
- deliberately access or disclose personal data or information without authority

Much of what appears online is, or claims to be, protected by copyright. If so, only the owner of the copyright is allowed to copy the information. Any copying without permission, including electronic copying, is prohibited. The copyright laws apply not only to documents but also to software. If in doubt over the copyright of an internet document, ask for advice from your line manager or the Chief Executive.

5 (b). Email

H4All CIO staff may need access to email to perform their duties. If so staff, volunteers, stakeholders etc. will be provided with a relevant organisational (H4All CIO or other provider) email address for correspondence.

Organisational email addresses should be used for business purposes only.

Email is inherently insecure. It must not be used to send confidential or sensitive information unless specifically authorised. Even then, appropriate security controls/encryption must be put in place.

All emails should be read on screen and users should only print those which need keeping for reference.

Email is not a substitute for face to face or telephone communication. Care must be taken that the content of messages cannot be misinterpreted.

The style and content of email messages must be consistent with the professional standards H4All CIO identify.

Statements made in emails must be factually correct and expressed appropriately.

Only relevant emails should be sent and the automatic forwarding of messages to long circulation lists, which unnecessarily increases the traffic and the time spent dealing with irrelevant correspondence should be avoided. Messages should only be cc or bcc when it is absolutely essential.

Do not use the “reply to all” facility incautiously or cascade “chain”, “junk” or “spam” emails to anyone else. Use the “reply” facility only when you have something specific to say.

Email boxes must be cleared on a regular basis.

Emails can be copied, cascaded or misdirected to people you did not intend to receive them. They may become contractually enforceable or even be used in legal proceedings against us.

Contracts can be offered, accepted and varied by exchange of email and may be binding. This can apply even if the sender does not have authority to conduct such activity on H4All CIO’s behalf.

H4All CIO are potentially liable for inaccurate, inappropriate or defamatory content circulated. H4All CIO hold staff/secondees/volunteers accountable for all email communications they initiate that may affect us. This applies whether what is said is contained in official or personal email(s).

H4All CIO cannot guarantee staff/secondee/volunteer privacy when using email communication (both internally and externally). H4All CIO reserve the right to access your email at any time. This includes periods of holiday or sickness. H4All CIO routinely monitor and review email usage to:

- reduce the level of inappropriate unsolicited email (spam) we receive
- manage our network to ensure our systems operate efficiently and securely
- identify unauthorised usage, including breaches of these rules and procedures
- prevent or detect crime
- intercept communications that may contain viruses
- monitor volume and nature of email whether sent individually or more generally
- establish information and produce statistics relevant to our operation
- determine whether or not communications relate to us

Line Manager(s) must be informed of any infringement of this policy or matters of concern can be raised formally by using Grievance or Whistleblowing procedure(s).

5 (c). Social Networking

Staff/secondees/volunteers should not make contributions relating to H4All CIO on social networking sites unless part of their role.

Staff/secondees/volunteers should not comment about any other employee, client, supplier, stakeholder etc. This applies to both use of H4All CIO or personal IT systems; whether in work time or non-work time. Such contributions may impact detrimentally upon our interests, whether inadvertently or otherwise. H4All CIO will view infringements as a serious breach of our rules. This may result in disciplinary action and, potentially, dismissal.

Where there is a genuine grievance about something at work staff/secondees/volunteers should not use social networking sites to pursue it. Staff/secondees/volunteers should discuss with Line Manager(s) at an early opportunity. H4All CIO also have a Whistleblowing system which is available to all employees. This provides an appropriate means of raising matters of concern about any aspect of our organisation.

5 (d). Security Rules

Staff/secondees/volunteers are responsible for the security of all IT systems provided for use.

All IT systems should be:

- logged off and powered down when not in use
- locked to prevent inappropriate access by others when not in use
- locked away securely when not in use
- not be left on view or unattended in vehicles

Only relevant information should be kept on IT systems.

Where electronic data entry is done in publicly accessible areas e.g. reception areas, the display screen for the IT system should be positioned in such a way so that others cannot see what is being displayed. If this is not possible then privacy screens should be used on the display screen to afford a level of protection.

Links to external websites that are made available through the H4All CIO website or in any of our publications are for the purpose of convenience or citation. H4All CIO is not responsible for the content or privacy policies of these other pages. Visitors are encouraged to review each site's privacy policy before disclosing any personally identifiable information.

It is not permitted to make use of loopholes on the Internet, or web sites' security systems to access, damage or alter any files held on any IT system or website.

5 (e). Passwords

Passwords must be:

- kept secure
- not divulged to any other person or organisation
- not written down
- not kept in a form which is easily identified
- not saved on IT systems
- not entered in view of others which would allow them entry to IT systems

If for any reason it is believed that someone has unauthorised access to passwords, you must inform your line manager and change it immediately. Failing to do so could leave you personally liable for any damage caused by someone accessing IT systems using your details.

5 (f). Viruses

Firewalls and virus protection are employed at all times to reduce the possibility of hackers accessing H4All CIO IT systems and thereby obtaining access to confidential records.

The introduction of a virus when downloading software/files from the Internet or within email messages poses a risk to all H4All CIO IT systems. Anti-virus software is installed on the server and relevant IT systems and must not be removed or disabled.

If an IT system is not connected to the H4All CIO server; any emails where the sender is not known to you/is obviously not to do with our line of work/the subject of the email has been left blank or has an attachment from an unknown sender; should not be opened.

All software should be obtained from controlled legal sources and no software should be installed or downloaded from the Internet without approval of the Line Manager or Chief Executive.

The deliberate introduction of viruses onto IT systems is an offence and, if proven, will be considered to be gross misconduct under the H4All CIO disciplinary policy.

5 (g) Accessing Personal Records

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information about themselves, their own family, friends or other persons without a legitimate purpose.

Under no circumstances should employees access records about themselves, their own family, friends or other persons without a legitimate purpose.

This applies to any and all IT systems utilised by H4All CIO staff whether in situ at H4All CIO or within GP surgeries.

Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 2018.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of NHS England and H4All CIO. If staff have concerns about this issue, they should discuss it with their Line Manager or DPO.

6: Confidentiality and Non-Disclosure

Confidentiality exists to offer protection of individual's right to privacy.

It is the policy of H4All CIO that all information regarding the organisation, clients, staff, volunteers, trustees, donors, contractors, suppliers and other relevant stakeholders should be treated, in the first instance, as confidential. This general principle applies throughout this policy unless an exception is clearly noted and/or H4All CIO are legally obliged to contravene this. This general principle also applies to all individuals who represent the organisation.

Information relating to the organisation should only be disclosed with the consent of the line manager or Chief Executive, as appropriate.

H4All CIO will not disseminate identifiable personal information/data about clients or employees apart from such information which is needed to be shared in order for staff to discharge their day to day duties; providing that consent had previously been given by the client, line manager or staff member.

Where H4All CIO must disclose information to comply with the law H4All CIO will do so under the lawful basis of 'Legal Obligation'.

Exemptions to this will be in the prevention or detection of crime, any possible abuse of vulnerable children or adults, or in relation to issues which may endanger public health or personal safety.

It may occasionally be appropriate for H4All CIO to disclose personal information about its employees when police checking. Such disclosures will be determined/authorised by the line manager or Chief Executive and in their absence by their deputy or, in the event of information concerning the Chief Executive, by the Chair of the Board of Trustees.

Members of staff have access to organisational data relevant to their roles and duties. All such information is regarded as confidential. Members of staff can only have access to information about other staff and clients for the discharge of their duties.

Volunteers are not permitted to access sensitive data unless they are deployed in a role in which processing of this data/knowledge of this data, is relevant. Trustees similarly are not permitted to access such data unless deployed in an appropriate additional role.

Confidential and personal information relating to staff, volunteers and clients will not be shared or discussed with anyone outside of H4All CIO e.g. friends, acquaintances or family.

Members of staff must observe the procedures and recording guidelines on the handling of information at all times. Failure to observe the requirements of Confidentiality and Non-Disclosure is likely to result in disciplinary action in accordance with other policies of H4All CIO.

All stakeholders are made aware that confidentiality principles extend to issues including face to face discussions, telephone conversations and other means of communications.

The above principles apply after a person ceases to be employed by or have association with H4All CIO.

6 (a). Client Confidentiality

H4All CIO aims to respect the confidentiality and dignity of all its clients. Personal details of individual clients, and details of their individual case are strictly confidential within the organisation, and must not be passed on to a third party or outside the organisation except with the client's express permission; except where there is a justifiable reason to believe that the client:

- is at serious risk of harming themselves, or others
- is intending to commit, or has committed, a criminal act
- is at risk of abuse or has been abused
- is a serious risk to society

H4All CIO must agree with the client how to deal with confidentiality in future communications e.g. when calling someone back it should be confirmed that the person they want is the person they are speaking to before advising they are from H4All CIO.

Staff should always request permission to read any documents given to them by a client or third party to emphasise the importance of confidentiality within H4All CIO. Any documents received from clients should be kept in a secure/lockable location and clients should be issued with a receipt for the documents.

Staff should be aware of limitations of locations away from the office as regards confidentiality as other members of the public are present.

Any information gathered from casework in the form of Case Studies should be recorded in a non-identifying manner so that the client's data remains confidential.

If an unknown third-party contacts H4All CIO without the knowledge of a client, H4All CIO is not authorised to take action on the client's behalf. Staff should attempt to gain direct contact, or if not practical, signed authorisation or should draft a letter for the client to sign and send.

Staff should be careful in their response to a direct question asked by a third party about a client. They should attempt to answer in such a way that does not enable the enquirer to form a definite opinion. When in doubt about how to handle personally or professionally any information received, workers should contact their line manager.

6 (b). Employee, Secondee/Volunteer Confidentially

6 (b1). Personnel records

Personnel records are held in accordance with the policies and procedures of the employee's parent organisation. Where appropriate or where H4All CIO becomes an employer, it will maintain a personnel record or nominate a lead partner to discharge the function on behalf of H4All CIO. This includes copies of post holder's application forms, salary details, appraisal records, copies of employment contracts, and any disciplinary records. Members of staff are entitled to have access to their copies of all of these documents with the exception of their references. A record of the emergency contact details for staff seconded to H4All CIO will be maintained in Charitylog/MyHR (or other relevant system) accessible by the Service Manager and Chief Executive(s).

6 (b2). References

References are held with a post holder's personnel records in accordance with the policies of the employing organisation. Should H4All CIO become an employer or recruit staff directly, these records will be retained by H4All CIO using Charitylog/MyHR (or other relevant system). References may be seen by members of the interviewing panel only. Request to consult references may only be made to the Lead Chief Executive.

6 (b3). Supervision and Appraisal Records

Supervision and Appraisal records are maintained in accordance with the employing organisations policies and procedures. Should H4All CIO become an employer, supervision and appraisal records will be agreed by the post holder and the signed copy held on the post holder's personnel file and an entry made on Charitylog/MyHR (or other relevant system). Supervision and appraisal records may not be seen by anyone other than the post holder, the post holder's line manager(s), Lead Chief Executive, and Directors with the agreement of the Lead Chief Executive.

6 (b4). Emergency Contact Records

Emergency contact records are held on Charitylog/MyHR (or other relevant system) and on the post holder's personnel file in accordance with the policy and procedures of the parent organisations. All staff should ensure that the person named on their emergency contact record has agreed to act in this capacity. In an emergency, any member of staff or secondee may have access to the contact records of an affected colleague. Outside of an emergency, the emergency contact form is understood to be confidential within the organisation.

6 (b5). Volunteer Records

Information shared by volunteers/prospective volunteers will be regarded as confidential within the organisation. Information held on volunteers should be accessed on a strictly need to know basis. Volunteers will be notified that personal records are kept on file.

Volunteer information about a prospective volunteer will not be shared with any external organisation without explicit consent to do so. H4All CIO is not a vetting agency and believes strongly in promoting volunteering opportunities for all, in accordance with H4All CIO Equal Opportunity policy. However, there may be occasions when H4All CIO is party to information which it is necessary to disclose as there is a justifiable reason to believe that the volunteer/prospective volunteer:

- is at serious risk of harming themselves, or others
- is intending to commit, or has committed, a criminal act
- is at risk of abuse or has been abused
- is a serious risk to society

In all cases, a decision to disclose should be taken after discussion with the Lead Chief Executive or, in their absence, one of the other CEOs comprising the CEO Group.

7: Accessibility

This notice can be made available in different languages and larger fonts. Please contact the H4All CIO office for further information.

8: How to Contact H4All CIO or make a Complaint

H4All CIO has appointed a DPO; Dalvinder Jammu, to oversee compliance with its data protection obligations.

If you have any questions about this policy, how H4All CIO handles your personal information, or feel that your data has been processed in ways that are not compliant with the information detailed in this policy, please contact the DPO at info@H4All.org.uk or write to H4All CIO on the details below:

H4All CIO The Data Protection Officer

Address: Key House | 106 High Street | Yiewsley | Middlesex | UB7 7BQ

Tel: 01895 54 34 34

Email: info@H4All.org.uk Website: www.H4All.org.uk

You also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK Supervisory Authority for data protection issues.

You can contact the Information Commissioner by Telephone: 0303 123 1113 (local rate) or by email at casework@ico.org.uk. Alternatively, you can write to:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

The Information Commissioner's website has more information about data protection and your rights; https://ico.org.uk/

9: Changes to the Information Governance Policy

H4All CIO keep our policies under regular review. This privacy notice was last updated on 30 October 2018.

10. Approval

This policy has been approved by the Charity Board of Trustees and will be reviewed on an annual basis.

Approved by	Charity Board of Trustees
Last reviewed	September 2019
Next date for review	September 2020

DATA RETENTION SCHEDULE

Category of Data	Purpose of processing	Primary Legal Basis for Processing	Retention Period	Disposal Activity
Client/Stakeholder Records				
Case Files/History Contact Forms	Providing service for data subject	Consent	**Digital:** Indefinitely for 'active' clients 2 years for 'inactive' clients **Hard Copy:** Indefinitely for 'active' clients 2 years for 'inactive' clients	**Digital:** Remove/Anonymise from CRM **Hard Copy:** Shredded
Case Files/History Contact Forms for Counselling Records	Providing service for data subject	Consent	**Digital:** Indefinitely for 'active' clients 7 years for 'inactive' clients **Hard Copy:** Indefinitely for 'active' clients 7 years for 'inactive' clients	**Digital:** Remove/Anonymise from CRM **Hard Copy:** Shredded
Case Files/History Contact Forms for Minors	Providing service for data subject	Consent	**Digital:** Indefinitely for 'active' clients 25 years for 'inactive' clients **Hard Copy:** Indefinitely for 'active' clients 25 years for 'inactive' clients	**Digital:** Remove/Anonymise from CRM **Hard Copy:** Shredded

Category of Data	Purpose of processing	Primary Legal Basis for Processing	Retention Period	Disposal Activity
Engagement with Stakeholders	Providing service for data subject	Consent	**Digital:** Indefinitely for 'active' clients 2 years for 'inactive' clients **Hard Copy:** Indefinitely for 'active' clients 2 years for 'inactive' clients	**Digital:** Remove/Anonymise from CRM **Hard Copy:** Shredded
Organisational				
Board minutes and papers	Legal Compliance	Legal Obligation	6 years from creation.	**Digital:** Remove from CRM **Hard Copy:** Shredded
Strategic Plan, Business Plan, Risks etc.	Legal Compliance	Legal Obligation	6 years from completion.	**Digital:** Remove from CRM **Hard Copy:** Shredded
Audit(s) and report(s)	Legal Compliance	Legal Obligation	6 years from completion.	**Digital:** Remove from CRM **Hard Copy:** Shredded
Data Protection and FOI complaints	Legal Compliance	Legal Obligation	6 months after case closure.	**Digital:** Remove from CRM **Hard Copy:** Shredded
Emails contained within archive	Legal Compliance	Legal Obligation	6 years (Best practice)	**Digital:** Remove from CRM
Policy and Communications	Legal Compliance	Legal Obligation	6 years from creation (Best practice)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Legal				
Provision of Legal advice	Legal Compliance	Legal Obligation	6 years from date of advice (Best practice)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Legal grant files	Legal Compliance	Legal Obligation	Asset liability period (Best practice)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Litigation with third parties	Legal Compliance	Legal Obligation	6 years after settlement of case (The Limitation Act 1980)	**Digital:** Remove from CRM **Hard Copy:** Shredded

Category of Data	Purpose of processing	Primary Legal Basis for Processing	Retention Period	Disposal Activity
Property Acquisition (purchase, donation, lease, rental, transfer, etc)	Legal Compliance	Legal Obligation	Ownership of property, asset liability period.	**Digital:** Remove from CRM **Hard Copy:** Shredded
Finance				
Payroll	Legal Compliance	Legal Obligation	6 years (Best practice) HM Treasury guidelines, National Audit Office advice, Companies Act 2006	**Digital:** Remove from CRM **Hard Copy:** Shredded
All other financial records	Legal Compliance	Legal Obligation	6 years from creation (Tax Management Act 1970, The Limitation Act 1980, Value Added Tax Act 1994, Companies Act 1985)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Grant Applications	Grant Application	Contract	7 years from end of grant and/or from decision for unsuccessful grants (liability period).	**Digital:** Remove/Anonymise from CRM **Hard Copy:** Shredded
Fundraisers/ Fundraising	Contract	Contract	2 years then refresh consent. For Gift Aid compliance 6 years	**Digital:** Remove/Anonymise from CRM **Hard Copy:** Shredded
Correspondence with Inland Revenue	Legal Compliance	Legal Obligation	Review every three years (Best practice)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Internal correspondence	Legal Compliance	Legal Obligation	1 year (Best practice)	**Digital:** Remove from CRM **Hard Copy:** Shredded
HR				
Employee Contracts Volunteer Agreements	Legal Compliance	Legal Obligation	12 years after termination (The Limitation Act 1980)	**Digital:** Remove from CRM **Hard Copy:** Shredded

Category of Data	Purpose of processing	Primary Legal Basis for Processing	Retention Period	Disposal Activity
Employee/Volunteer Files, Training and Personal Development records	Legal Compliance	Legal Obligation	6 years from date of employment end (Best practice)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Disciplinary and Grievance, Absence and Ill health	Legal Compliance	Legal Obligation	6 years from date of employment end (Best practice)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Maternity, Paternity, Adoption and Sick Leave	Legal Compliance	Legal Obligation	6 years (Best practice) Statutory Sick Pay (General) Regulations 1982 Statutory Maternity Pay (General) Regulations 1986 Statutory Paternity and Statutory Adoption Pay (Administration) Regulations 2002	**Digital:** Remove from CRM **Hard Copy:** Shredded
DBS records	Legal Compliance	Legal Obligation	6 months following recruitment	**Digital:** Remove from CRM **Hard Copy:** Shredded
Job/Volunteer applications and interview records for unsuccessful applicants	Legal Compliance	Legal Obligation	6 months after notifying unsuccessful candidates (Sex Discrimination and Race Relations Acts)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Personal exposure to hazardous materials by employee	Legal Compliance	Legal Obligation	40 years from incident (Best practice)	**Digital:** Remove from CRM **Hard Copy:** Shredded
Insurance: - public liability - product liability - employer's liability	Legal Compliance	Legal Obligation	Life of the organisation.	**Digital:** Remove from CRM **Hard Copy:** Shredded
Health policies/Personal accident policies	Legal Compliance	Legal Obligation	12 years after cessation of benefit (The Limitation Act 1980)	**Digital:** Remove from CRM **Hard Copy:** Shredded

Category of Data	Purpose of processing	Primary Legal Basis for Processing	Retention Period	Disposal Activity
Buildings and Facilities				
Sign in books	Legal Compliance	Legal Obligation	2 years (Best practice)	**Hard Copy:** Shredded
CCTV	Legal Compliance	Legal Obligation	1 month	Erased