CHUMS

Mental Health and Emotional Wellbeing Service for Children and Young People

Information Governance Policy

Implementation Date: May 2017

Revised May 2018

Review Date: May 2021

CHUMS
Mental Health & Emotional Wellbeing Service
For Children & Young People
Information Governance Policy

CONTENTS

Introduction and Background

This policy will outline CHUMS approach to Information Governance which seeks to ensure that information held by CHUMS is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care to clients.

Implementation of this policy will ensure all staff comply with the law and best practice when handling personal and corporate information.

The national Information Governance Toolkit was launched by the Department of Health in November 2003. The Toolkit enables CHUMS to measure itself against nationally agreed standards.

The Toolkit provides a framework comprising of Department of Health guidance, compliance with information management legislation and year on year improvement plans.

The Information Governance framework will enable CHUMS to meet its legislative requirements, and ensure operational and management information is timely, robust and reliable.

Full implementation of this policy will ensure all staff comply with the law and best practice when handling personal and corporate information.

The key drivers of Information Governance are to:

- Protect clients and staff
- Meet legislative requirements
- Ensure comprehensive, timely and accurate information at all levels
- Comply with CHUMS risk management procedure
- Make compliance as easy as possible for staff while providing a good level of training and awareness

CHUMS will ensure that all staff are aware of this policy, particularly in relation to their own responsibilities. Staff must also familiarise themselves with other related Information Governance policies. These are:

- Information Sharing Policy
- Information Sharing Protocol
- Documentation Policy
- Confidentiality and Disclosure Policy
- Record Management Policy
- Clinical Records Policy
- Risk Assessment Policy

- Data Protection Policy
- Adverse Incident – Serious Incident Reporting Policy
- Parental Consent Policy
- Freedom of Information*

  * Although this legislation does not directly apply to CHUMS as it is not a public body, requests for information may come via the NHS Community Services and other public bodies where CHUMS is contracted to provide services.

Information Governance (IG) supports and underpins the governance arrangements within CHUMS, including clinical, research, corporate and financial governance.

IG is a CHUMS wide issue. To develop information governance within CHUMS there are broadly five areas that need to be addressed:

- Policies
- Training
- Operational Practices
- Audit/compliance
- Performance Measurement.

IG encompasses seven key areas:

- Information Governance
- Clinical Information Assurance Management
- Confidentiality and Data Information
- Security Assurance
- Protection Assurance
- Corporate Information Assurance
- Secondary Use Assurance

IG covers:

All clients	All staff including volunteers
Information in any format	Health and corporate administrative records
Current and future IT systems	Relationships with external organisations

The Policy

This policy sets out that information must be:

- ***Held Securely and Confidentially***
- ***Obtained Fairly and Efficiently***
- ***Recorded Accurately and Reliably***
- ***Used Effectively and Ethically***

- ***Shared Appropriately and Lawfully***

Held Securely and Confidentially
Staff must ensure that all personal, sensitive and corporate information is held securely and confidentially. CHUMS systems demonstrate the importance CHUMS places of the security of client information.

Staff must ensure that all information is kept secure, either through the use of an individual username and password, which must not be shared or used by another member of staff, by keeping information in locked filing cabinets or transporting information (client case-notes) securely. (See CHUMS Information Sharing policy.)

Staff must ensure that all information is stored correctly on a CHUMS network drive, stored using correct filing structures and names. CHUMS undertakes comprehensive back up arrangements for all CHUMS data; therefore it is imperative all information is stored on the CHUMS network drives.

Staff must ensure that information is only kept for as long as necessary (General Data Protection Regulations GDPR 2018) and when no longer needed is disposed of in accordance with CHUMS Records Management Policy using secure and confidential destruction methods.

Information Governance incidents of actual or potential breaches of confidentiality and security must be reported and investigated following CHUMS Adverse Incident – Serious Incident Reporting Policy.

Obtained Fairly and Efficiently
Staff should consider situations in which clients would be surprised to learn that their personal information was being used in a particular way – if so, they are not being effectively informed
Clients must be:

- Informed of how CHUMS uses their information e.g. research, training, audits etc.
- Given the opportunity to ask questions on how their information is used and with whom it is shared

Staff must ensure that when a client decides to restrict the disclosure of their personal information, this decision is respected *and* recorded appropriately.

CHUMS will develop effective procedures for ensuring that questions raised by clients about how their information is used by CHUMS are answered.

Recorded Accurately and Reliably
CHUMS will develop procedures for staff on the capture and recording of information. All staff must ensure they familiarise themselves with and follow these procedures. See CHUMS Records Management Policy and Clinical Records Policy for further information.

CHUMS aims to collect all client information once and ensure that at this point of collection; the information is accurate and up to date.

CHUMS will ensure that all data standards will be set through clear and consistent definition of data items, in accordance with national standards.

CHUMS will promote information quality and effective records management through policies, procedures/user manuals and training.

In order to assure itself as to the quality of the information collected, CHUMS will undertake regular accuracy, completeness and validity checks on client information with 6 monthly clinical records audits.

Used Effectively and Ethically
CHUMS will ensure that all staff access to client information is based on a legitimate relationship between the client and the member of staff.

Shared Appropriately and Lawfully
The Freedom of Information (FoI) Act 2000 is part of the Government's commitment to greater openness and transparency in the public sector.

The Act provides members of the public with a general right of access to recorded information held by public authorities, subject to certain conditions and exemptions. Staff have a legal obligation to provide guidance and assistance to a person wishing to make a request under FoI for any corporate information.

CHUMS primarily collects and holds clients' information in relation to their care, but is holding this information on behalf of the client. Clients, and any other individual about whom CHUMS holds information, have a legal right to access information relating to themselves held by CHUMS.

Comprehensive Subject Access Request procedures (see CHUMS Data Protection policy and Parental Consent policy) provide clear guidance to staff on how to deal with requests from individuals to access their information.

CHUMS has a legal obligation to ensure that all requests from individuals to access their information are dealt with *within forty calendar days* from the date of the request.

CHUMS has a legal obligation to actively inform clients of how their information is used, give them the choice to give or withhold their consent on how their information is used and protect their identifiable information from unwarranted disclosure.

Protocols and policies have been established for controlled and appropriate sharing of client information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act) - see CHUMS Information Sharing Policy.

Staff must follow the standards and procedures set out in this protocol when disclosing confidential client information to organisations and agencies.

Staff who share information with other NHS organisations must ensure they attend relevant training sessions.

Staff must ensure that when sharing information, the Caldicott principles are applied. These are:

- Justify the purpose(s) of using confidential information
- Only use it when absolutely necessary
- Use the minimum that is required
- Access should be on a *strict* need to know basis
- Everyone must understand his or her responsibilities
- Understand and comply with the law
- The duty to share can be as important as the duty to protect patient- client confidentiality

Staff must obtain explicit consent from all clients before transferring their information outside of the EEA (European Economic Area). Whilst obtaining consent, CHUMS will ensure that the client is fully informed on how their information is used.

Roles and Responsibilities

The Board has overall responsibility for CHUMS compliance with Data Protection. The Operational Director is the nominated responsible officer for CHUMS for information governance together with matters regarding FoI (Freedom of Information) and PRA (Public Records Acts) although as CHUMS is not a public body these acts are not directly applicable.

The Operational Director supported by CHUMS Risk and Security Lead and CHUMS Governance Projects Lead make up the IG team, being SIRO, Data Protection Officer and Caldicott Guardian respectively. The IG team are a part of

the Governance Committee which oversees both clinical and information governance across the organisation.

Implementation

CHUMS is developing an Information Governance strategy, which will be reviewed annually and include an annual improvement plan.

A designated Senior Clinical Psychologist or BACP accredited Psychotherapist chairs the CHUMS Governance Committee. The group meets and reports to the CHUMS Board on a quarterly basis.

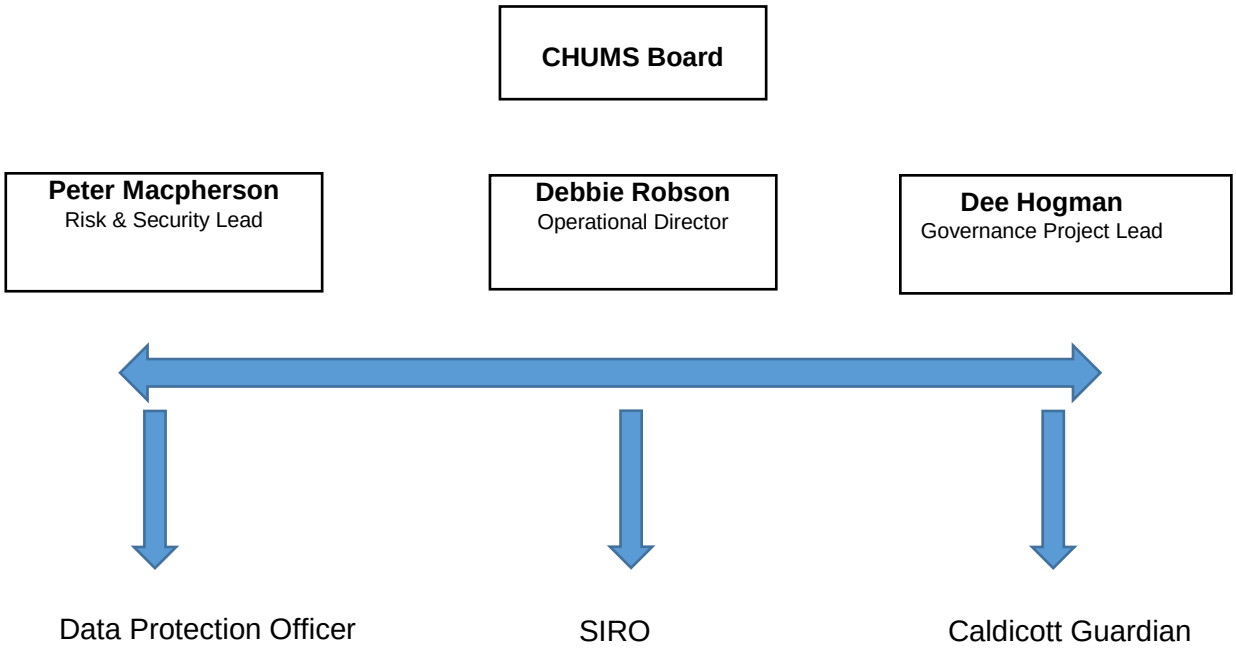
The Governance Committee is responsible for ensuring detailed annual action plans are developed and implemented to ensure that all IG requirements are met:

Staff Training and Support

The Lead for Information Governance will develop and implement a CHUMS wide training programme to ensure awareness and compliance by all staff for all Information Governance requirements.

Policies within CHUMS M: Drive will provide staff with detailed information and advice on all aspects of Information Governance.

Information Governance Management Structure



Governance Committee

Dr Julian Marsden - GP

Lizzie Mitchell - Acting EWS Manager (CHAIR)

Dee Hogman - Governance Projects Lead

Debbie Robson - Operational Director

Niki Scott – Service User Participation Officer

Pete Macpherson – Risk & Security Lead

APPENDIX A

Information Governance Code of Conduct

CHUMS *takes information security seriously and ensures that staff are aware of their responsibilities when handling all information that should be kept confidential.*

Information is required to look after clients and manage services resources. It is also import for: Clinical Governance (corporate accountability for clinical performance) Corporate Governance (meeting standards of accountability and integrity), service planning and performance management

We must manage information securely, efficiently and effectively, so we need suitable policies, procedures and management accountability to create a sound governance framework for information management.

All staff are required to read and sign this document

Confidential information can be anything that relates to clients (e.g. health records, complaints, and serious untoward incidents), staff or any other person, held either on paper or electronically. Confidentiality is a general legal requirement that applies to all CHUMS staff when handling personal information about others as part of their job.

There are many ways in which confidentiality could be breached, few are listed below this is not an exhaustive list;

- Accessing records you have no legitimate reason to see, for example your relatives and friends health records, even with their consent (unless it is within you job role to deal with such requests);
- Displaying information in a way that unauthorised people could see items;
    - Leaving workstations unlocked;
    - Leaving records open, unattended or insecure;
- Confidential Information disposed of inappropriately;
- Holding conversations about individuals where others could overhear
- Giving out confidential information in person, over the telephone, by fax or email to unauthorised people. When using emails, always double check that you are contacting the correct recipient, that any attachments are correct and appropriate. Always use a NEW email instead of reply in case earlier emails in the stream may lead to a data breach.

Failure by staff to comply with these guidelines and CHUMS policy may lead to disciplinary action.

Transfer of Person Identifiable Data (PID)[1] a. Portable Devices[2]

[1] Portable devices should be used as transitional tools for PID only when absolutely necessary for work purposes. The use of any of these items will constitute a risk as they are highly susceptible to loss.

- Ensure the whole device is encrypted wherever possible. Contact IT Support to arrange
- Store only the minimum amount of PID necessary for the current purpose on the device
- Store PID only for the time period when it is actively used

Person-identifiable data (PID) covers client or staff information and can include the following:

- Name, address, full postcode, date of birth, financial details of clients or staff
- Pictures, photographs, videos, audio-tapes or other images of clients; copies of passports, birth certificates of staff
- NHS number and local client identifiable codes; national insurance number or payroll number of staff
- Anything else that may be used to identify an individual directly or indirectly, e.g., rare diseases, drug treatments or statistical analyses with very small numbers within a small population

[1] Portable devices can include, laptops & handheld computers, Mobile phones, Tablets and other mobile devices, optical discs (DVD / CD), solid state memory cards and memory sticks. As technology changes this is not an exhaustive list.

- Delete PID from the device immediately after use
- Ensure the device is physically secure when unattended
- Whilst working on CHUMS site use the CHUMS network not a portable device or the local hard drive to store data
- Do not use portable devices for permanent storage of data. Any data on the device should be backed up on the CHUMS network

Post/Courier

- Send PID in a sealed envelope and mark it as “Private and Confidential”
- The envelope must display the recipient’s name, job title and full contact details
- To transfer sensitive or bulk data, use special delivery (tracked) by post or a courier
- If using a courier ensure that CHUMS has a contract with the courier company

- Include a return name and address in the top left hand corner on the back of the envelope

Email

- When emailing within the organisation ensure PID is sent between CHUMS accounts: @chums.uk.com
- Do not use personal email accounts (e.g. Hotmail) to send or receive PID
- All bulk transfers of PID should be approved by the IG team before commencement then sent via secure file transfer
  This is under review

Telephone

Disclosure of PID via telephone should be the exception rather than standard practice

- Always confirm the identity of the other party before disclosing information
- Dial back arrangements should be used to ascertain the person is authorised to receive the data
- The member of staff should ensure that they know the reason why the other party requires the information
- Recorded telephone messages must be received into a secured, password protected voicemail box
- For times of absence, a deputy should be appointed and an administrator password made available
- Any log books used to record phone messages should be stored securely

Fax

When faxing PID, a safe haven fax[1] should be used. If you are unsure whether the machine you are using is a safe haven fax or not, use the following procedures:

- Anonymise PID wherever possible. If this is not possible, use NHS number instead of name, DOB etc
- Telephone the recipient of the fax to let them know you are sending them PID
- Always double check the fax number before you hit the send button
- The cover sheet should state who the information is for and be marked "Private and Confidential
- Request a report sheet to confirm that the transmission was successful
- If necessary, contact the recipient to ensure they have received the fax
- Never leave the fax machine unattended whilst the fax is being transmitted

[1] Safe haven faxes are faxes located in a secure office which is always locked when not in use/occupied and all received faxes are to a named individual and are dealt in a timely fashion.

Records Management

- Do not store confidential CHUMS data on the M: drive or desktop; us a secure/restricted shared drive folder, your H drive (where appropriate), or approved CHUMS software (e.g. PCMIS©)
- When not in use always lock paper-based information securely away
- Emails containing PID must be filed appropriately on receipt e.g. in the health record or staff file and then deleted from the mailbox
- Information should be disposed of in accordance with the CHUMS Records Management policy and only in confidential waste bins

Laptops

All CHUMS laptops should be encrypted, and the guidelines for portable devices apply (see section 1a). PID should only be stored on a laptop when absolutely necessary for work purposes, and good practice guidelines for securing your laptop are as follows:

- When using a laptop to store PID:
    - Always lock it (**CRTRL+ALT+DEL)** when you leave your desk
    - When you are transporting or not using the device make sure it is switched off
- Do not leave laptops in insecure areas and use lockable rooms and storage facilities where available
- Take extra care of laptops used or transported in busy public places
- Carry laptops in protective anonymous bags or cases (i.e. without manufacturer logos)
- When travelling ensure that laptops are stored securely out of sight, but avoid placing them in locations where they could be easily forgotten e.g. overhead racks

More Information

Further information is available as follows:

- Data Protection Policy
- Information Sharing Policy
- Information Sharing Protocol
    - Confidentiality & Disclosure Policy
- Retention & Disposal Policy
- Freedom of Information Act
- Information Governance Quick Reference Guide
- FAQs

For advice and guidance contact the Information Governance team:

Information Governance incidents (e.g. loss of information, breaches of confidentiality) must be reported in line with CHUMS Adverse Incident-Serious Reporting policy and to the Information Governance Team immediately.

Declaration – to be signed by all staff and volunteers

I have read and understood the above information and will handle confidential information in line with CHUMS Policies, the Data Protection Act 1998 from 25th May 2018 General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

I understand that my failure to comply with these guidelines and CHUMS policies may lead to disciplinary action being taken against me.

Name
……

Signature
……..

Service
……..

Date
……

Please sign and return to HR Lead

Further Guidance

- The Data Protection Act 1998 from May 2018 General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000 and the supporting Codes of Practice
- Section 251 National Health Service Act 2006
- Confidentiality: NHS Code of Practice. Records Management: NHS Code of Practice ISO 17799 Information Security
- Caldicott Guardian Manual 2010
- The Computer Misuse Act (1990)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Public Records Act 1958

Appendix B

IG Guidance for Staff Managing Personal Information

Introduction

All CHUMS staff have a responsibility for managing and sharing information appropriately and in ways that comply with legal requirements. This includes all personal information, which is covered by the Data Protection Act and which must be handled in a way that protects the confidentiality and rights of individuals.

The following guidance is designed to help staff understand how personal information is defined, how it should be handled and the restrictions that apply.

- ***If you are unsure, please always seek advice from line manager before providing any information***

What is 'personal information'?

Personal information (also known as person identifiable data – PID) incorporates:

- Everything that could identify an individual – e.g. home address, National Insurance number, salary, etc.
- Any opinions expressed by or about an individual
- The intentions of someone else regarding an individual

The General Data Protection Regulation defines the following types of information as being particularly sensitive personal information – which must never be shared without consent:

- An individual's racial or ethnic origin
- His/her political opinions
- His/her religious beliefs or other beliefs of a similar nature
- Whether he/she is a member of a trade union (within the meaning of the **M1** Trade Union and Labour Relations (Consolidation) Act 1992)
- His/her physical or mental health or condition
- His/her sexual life and orientation
- The commission or alleged commission by him/her of any offence
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

What are the restrictions that apply to the handling of personal information?

Under the Data Protection Regulations state, any person referred to in any data has legal rights over the use of that data and that data should, therefore, not be shared without their consent.

Who does personal information apply to?

The same definitions and restrictions relating to personal information apply to all individuals for whom CHUMS, or individual employees, hold information. These include:

- All staff
- All tenants
- All customers
- All service users and their families
- And all others

The following conditions apply to the managing and sharing of personal information:

- Personal information held by CHUMS is held for specific officially registered purposes only
- The use of sharing of personal information for other purposes could be breaking the law
- All CHUMS staff are personally responsible for ensuring that any information shared with others does not breach the Data Protection Regulations, NHS Code of Confidentiality or other laws and codes
- If you share information with someone outside the company and that person uses the information in a way that breaches the Data Protection Regulations, you and the company remain accountable

Information that is NOT personal

In the case of an employee, information that relates to certain aspects of their employment is not classed as personal – including:

- Work contact details
- Job description
- Employee number
- Decisions they have made as part of their role (e.g. recorded in the minutes of a meeting)

What should I do if someone asks me for personal data relating to another person?

Personal information that is provided by an individual should only be used for the specific purpose for which it has been provided. For instance, employees provide HR with their bank account details for use by payroll only. This information cannot be provided to anyone else or used for any other purpose.

If someone asks you for information about another individual – whether the person asking is someone inside the organisation – such as by another member of staff (internal requests) or someone outside the company (external requests) – you need to make sure it is appropriate to share it.

In some cases, you can seek consent from the person who is in the data. However, this is not always possible or desirable (for example if the information has been formally requested in order to investigate possible fraud or by a body with statutory powers such as the police or HM Revenue and Customs).

Responding to internal requests for information

If someone from within the company asks you for information about someone else, you should always ask:

- Do you understand what they do?
- Why do they need the data?
- Does the purpose for which they want the information match the purpose for which the information was provided?
- Could they manage with less information than they are asking for, or could you anonymise it by removing any information that could be deemed to be personal?

- ***If you are unsure, please always seek advice from your line manager before providing any information***

Responding to external requests

All requests from any individual for personal information about themselves should be treated as a subject access request under the Data Protection Regulations.

Any request from any person for any other information about the company or its business should be referred to the Operational Director. This will be treated as a freedom of information request under the Freedom of Information Act (2000).

The release of personal data to outside companies/organisations is only permitted in situations where the company has a contract and/or data processing agreement in

place to ensure they only use the data for the purpose specified.

- ***If you are unsure, please always seek advice from your line manager before providing any information***

More information

- For further guidance on the handling of personal information and/or other aspects of information governance, please contact Debbie Robson Operational Director, Information Governance Lead, by email to debbie.robson@chums.uk.com

- You can find more information on the Data Protection Act 2018 at: M:\Projects\Information Governance

    - M:\Projects\Data Protection inc. GDPR

    - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Appendix C

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement**	**Notes**
Senior Roles	• Senior Information Risk Owner (SIRO): Operational Director • IG/SIRO Support: Risk & Security Lead (Data Protection Officer) • Governance Project Lead Caldicott Guardian	Due to the size of CHUMS some roles are combined
Key Policies	• Information Sharing policy • Documentation policy • Confidentiality and Disclosure policy • Records Management policy • Clinical Records Policy • Risk Assessment policy • Data Protection policy • Adverse Incident – Serious Incident reporting Policy • Parental Consent Policy • Duty of Candour	
Key Governance Bodies	**Board** • CEO • Operations Director • Risk & Security Lead	
Resources	• CEO • Operations Director • Clinical Director • Finance Director • HR-Admin Lead • Risk & Security Lead	
Governance Framework	• Staff Induction and Training • Contracts of Employment • Related Policies (above) • Managers and Departmental Heads • This should include staff contracts, contracts with third parties, Information Asset Owner arrangements, • Departmental leads	
Training & Guidance	• Staff Code of Conduct • Training for all staff • Organisation Security Policy	

	• Training for specialist IG roles • All relevant policies	
Incident Management	• Adverse Incident – Serious Incident reporting Policy	

Authorised

Signature **Name (print)** **DAWN HEWITT**

Position within CHUMS **CHIEF EXECUTIVE OFFICER** **Date**

CHUMS
Mental Health & Emotional Wellbeing Service
For Children & Young People
Information Governance Policy

Governance Committee Authorisation

Signature * 

Name Print: Hannah Baron

Position/Role: Senior Clinical Psychologist

Date: May 2018

Date of Review: August 2021