CHUMS

Mental Health &
Emotional
Wellbeing Service

E-Safety Policy

Implementation Date: September 2017

Reviewed: January 2026

Review Date: January 2029

CONTENTS

E Safety Policy

1. Introduction

CHUMS recognises that the internet and other digital technologies provide a vast opportunity for children and young people to learn and share information. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the health and emotional wellbeing of children and young people to promote creativity, stimulate awareness and enhance understanding.

As part of our commitment to support children and young people to reach their potential we want to ensure that the internet and other digital technologies are used to enable children and young people to gain access to a wide span of knowledge in a way that ensures their safety and security.

To enable this to happen we have taken an organisation wide approach to E-safety which includes the development of policies and practices, education and training, of staff and young people and the effective use of the organisation's infrastructure and technologies.

CHUMS is committed to ensuring that all children and young people will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

The nominated senior person for the implementation of the organisation's E- safety policy is the Operations Director.

2. Scope of Policy

The policy applies to:

- all children and young people supported by CHUMS
- all staff and volunteers
- parents/carers
- professionals

CHUMS will ensure the following elements are in place as part of its safeguarding responsibilities to service users and their families:

- a list of authorised persons who have various responsibilities for E-safety
- a range of policies which are frequently reviewed and updated
- information to parents that highlights safe practice for children and young people when using the internet and other digital technologies
- adequate training for staff and volunteers

- adequate supervision of children and young people when using the internet and digital technologies
- guidance that is aimed at ensuring safe use of internet and digital technologies;
- a reporting procedure for abuse and misuse.

3. Policies and Procedures

CHUMS understands that effective policies and procedures are the backbone to developing an organisation wide approach to E-safety. The policies that exist at CHUMS are aimed at providing a balance between exploring the potential of new technologies and providing safeguards to children and young people.

3.1 Use of internet facilities, mobile and digital technologies

CHUMS will seek to ensure that internet, mobile and digital technologies are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk.

CHUMS expect all staff to use the internet, mobile and digital technologies responsibly and strictly according to the conditions below. CHUMS staff will encourage parent/carers to adopt these responsibilities when advising their children.

Users shall not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
- Indecent images of children
- Promoting discrimination of any kind e.g. promoting racial or religious hatred, promoting illegal acts
- Any other information which may be offensive

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police. Examples include:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy

- Other criminal activity

<u>In addition, users may not:</u>

- Use the broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves CHUMS in any way;
- Visit sites that might be defamatory or incur liability on the part of CHUMS or adversely impact on the image of the organisation;
- Upload, download or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
  - Financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate
- Transmit unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe
- Assist with unauthorised access to facilities or services
- Undertake activities with any of the following characteristics:
  - Wasting staff effort or networked resources, including time on end systems accessible via the network and the effort of staff involved in support of those systems
  - Corrupting or destroying other users' data, violating the privacy of other users, disrupting the work of other users
  - Using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)
- Continuing to use an item of networking software or hardware after request to cease because it is causing disruption to the correct functioning of the network
- Other misuse of the network, such as introduction of viruses

- Use mobile technologies (e.g. 5G, 4G, 3G or mobile internet services) in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal

3.2 Reporting Abuse

The following outlines what to do if a child or adult receives an abusive message or accidentally accesses a website that contains abusive material:

The abusive material should be stored, screenshot if possible and a copy sent to the relevant manager. The address (e.g. URL or email) linked to the abuse should also be recorded. However, the screen displaying the abusive material should be hidden from view and/or closed down as soon as possible to avoid further offence. The Adverse Incident Form should be filled out alongside this and given to the relevant manager in the first instance, within the stated time period.

4. Infrastructure and Technology

4.1 Partnership working

CHUMS recognises that as part of its safeguarding responsibilities there is a need to work in partnership. Our landlord, Wrest Park Estates and Facilities Department monitor network and broadband usage. As part of our commitment to partnership working, we fully support and will continue to work with our providers to ensure that children, young people and staff usage of the internet and digital technologies is safe.

5. Standards and Inspection

CHUMS recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to children and young people are minimised.

5.1 Monitoring

Monitoring the safe use of the internet and other digital technologies goes beyond the personal use of the internet and electronic mail a young person or member of staff may have. CHUMS recognises that in order to develop an effective organisation wide E-safety approach there is a need to monitor patterns and trends of use inside the organisation.

With regards to monitoring trends, within the organisation and individual use by staff, children and young people, CHUMS will audit the use of the internet and electronic mail in order to ensure compliance with this policy. CHUMS will also work with its internet service provider to further ensure compliance.

Another aspect of monitoring, is the use of mobile technologies by children and young people, particularly where these technologies may be used to cause harm to others, e.g. bullying. We will also ensure that staff understand the need to support individuals where they have been deliberately or inadvertently subject to harm and, in such cases, follow relevant policies and procedures.

5.2 Sanctions

Where there is inappropriate or illegal use of the internet and digital technologies, the following sanctions will be applied:

Child / Young Person

Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance in the event of, illegal Internet use or safeguarding concerns

Adult (Staff and Volunteers)

The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy

Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance in the event of, illegal Internet use or safeguarding concerns

6 Data Protection

CHUMS processes personal data collected during the implementation of this policy, in accordance with its data protection policy. Any data collected is held securely and accessed by, and disclosed to, individuals only for the purposes of inspecting, monitoring and reviewing the safe use of the internet and other digital technologies. Inappropriate access or disclosure of employee, child or volunteer data constitutes a data breach and should be reported in accordance with CHUMS' data protection policy immediately. It may also constitute a disciplinary offence, which will be dealt with under CHUMS' disciplinary policy and procedure.

7 References to other policies

E Safety Policy

Adverse Incident – Serious Incident and Reporting
Communications Policy
Cookies Policy
Data Protection Policy
Disciplinary Policy
Safeguarding Children Policy
Social Media Policy
Whistleblowing Policy

CHUMS
Mental Health & Emotional Wellbeing Service

E Safety Policy

Governance Committee Authorisation

Signature	Denise Hogman
Name Print:	Dee Hogman
Position/Role:	Head of Quality, Chair of Governance Committee
Date:	January 2026
Date of Review:	January 2029

Policy discussed and ratified at the Clinical & Information Governance meeting held on 29/01/2026. Quorum was reached and specialist consultation was provided prior to the meeting by Jo Tredgett, external HR Consultant. As Chair, I state this process has taken place to ensure safe and robust working practices.

*Authorised signatory must be the chair (or deputising chair) of Governance Committee