Acceptable Use Policy

Date Approved: 31/10/2025
Approved by: SIRO
Version: 13.0

Next Review Date: 31/10/2026
Owner: Information Governance and Data Protection Officer

Document Version Control

Version Number	Change/Update	Author/Owner	Date
1.0	N/A	Ava Wieclawska and Lesley Taylor	Jun 2013
2.0	Removal of reference to posting humorous comments at 7.3.	Ava Wieclawska	Sep 2013
2.1	Minor reformatting; slight rewording; addition of reference to not linking to children and families on social networking sites and informing the AST if contacted by children or families.	Ava Wieclawska	Feb 2014
2.2	Review period extended from 6 months to 2 years. Acceptable Use Policies for panel and AST members and Clerks, and staff and Board members, combined into one policy. Addition of email management guidance at 4.6-4.8.	Ava Wieclawska	Jun 2014
2.3	Policy reviewed by Audit and Risk Management Committee (ARMC) – no changes recommended.	Ava Wieclawska	Aug 2014
3.0	Final policy approved by the CHS Board.	Ava Wieclawska	Aug 2014
3.1	Minor amendments to section 4.6 and to reflect revised job titles	Ava Wieclawska	Mar 2015
4.0	Final policy approved by SMT	Ava Wieclawska	Mar 2015
4.1	Removal of section 4.8	Ava Wieclawska	May 2015
6.0	Final policy approved by SMT	Ava Wieclawska	May 2015
6.1	Policy reviewed with a focus on sections on online communication including the use of CHIRP and social media and the electronic communication of sensitive information. Other minor amendments include to terminology.	Callum Morrison	Jun 2016
6.2	Minor amendments to terminology	Ava Wieclawska	Jul 2016
6.3	Amendments to terminology and social media guidance in line with CEO comments	Callum Morrison	Oct 2016
7.0	Final Policy Approved by CEO	Alice Wilson and Callum Morrison	Jan 2017
7.1	Changes made to terminology for GDPR and minor updates to procedure.	Callum Morrison	Aug 2017
7.2	Changes made to terminology for GDPR and minor updates to procedures & Panel Pal	Ellie Robertson	Jan 2018
7.3	Further checks for GDPR, prior to sending to SMT to approve.	Alice Wilson	Feb 2018
8.0	Approval of revisions	Alice Wilson	Mar 2018
8.1	Amendments to enable Outlook App mobile access to CHILDREN'S HEARINGS	Lynne Harrison	May 2018

9.0	Final Policy Approved	Lynne Harrison	May 2018
9.1	Amendments to incorporate new digital system requirements throughout	Katie Crone Barber	Jan 2020
9.2	Removal of One Drive requirements (no longer in scope)	Katie Crone Barber	Jan 2020
9.3	Changes to formatting, incorporation of Teams	Katie Crone Barber, Lynne Harrison, Sarah Hunter-Argyle	Feb 2020
10.0	Approval of revisions	Katie Crone Barber	25/02/2020
11.0	Revisions of relevant policies, email addresses, key terms	Sophie-Elise Anker	08/12/2023
12.0	Revisions to incorporate new technologies, updates to policies and job roles, and amendments to email address.	Danielle Metcalfe	11/09/2024
12.1	Policy amended to fit new policy template. Minor amendments to wording for clarity and correction of grammar.	Morrigan Seiles	30/10/2025
12.2	Updated to incorporate technological developments, amendments to roles.	Danielle Metcalfe	30/10/2025
13.0	Policy approved by SIRO.	Danielle Metcalfe	31/10/2025

Contents

1. Definitions 5
2. Purpose 5
3. Scope 6
4. Unacceptable Use 6
5. User IDs and passwords 7
6. Use of email systems 7
7. Use of personal, mobile and removable devices 10
8. Use of social media and messaging applications 11
9. Use of Microsoft Teams 13
10. Use of OneDrive 15
11. Use of IT and Communications Equipment 16
12. Use of the internet 17
13. Breach of this policy 17
14. Monitoring and review 18
15. Implementation, Communication and Compliance 18

1. Definitions

1.1 The definitions below are to help with the understanding of this policy and other similar documents.

Users	*CHS Community: CHS volunteers, CHS staff, Board members, Experts by Experience, Clerks (and their teams) and third-party suppliers/contractors with access to CHS information and/or systems.*
Systems	*The Community Hub and associated web-based apps and systems that provide full services to all users, including but not limited to CSAS, Outlook, Learning Academy.*
Device	*All IT equipment (except SCOTS equipment) used to gain access to CHS's systems (including, but not limited to, mobile phones, laptops, desktop computers, iPads and tablets.)*

2. Purpose

2.1 The Acceptable Use policy has been produced to protect the CHS Community and its partners from harm caused by the misuse of our Information Technology (IT) systems and information.

2.2 This policy defines the ways in which CHS's online systems, and all information generated using any CHS systems, must be used on personal or provided devices.[1] It also identifies the key risks of misuse and informs users of their responsibilities. Please note that acceptable use of the SCOTS network, used by CHS National Team members, is defined in the Scottish Government IT Code of Conduct.[2]

2.3 This policy also outlines the expectations for the CHS Community regarding the use of devices provided to them to undertake their responsibilities during their time with CHS.

2.4 For personal data and sensitive personal data held within these systems, CHS is the Data Controller and has a legal obligation to ensure that it is maintained securely at all times. Users must be vigilant when using IT equipment or mobile devices to access CHS systems.

[1] CHS systems include the Community Hub, email and MS Teams and all systems included in the Microsoft Office 365 suite.

[2] The IT Code of Conduct provides guidance on the use of SCOTS (Scottish Government Information Technology Network system) and, in particular, email and the use of the internet. The code applies to all users of the SCOTS system (including all CHS staff).

2.5 The policy forms part of CHS's wider Information Governance Policy Framework, which also includes CHS's Data Protection Policy, Information Security Policy and Records Management Policy.

3. Scope

3.1 This policy applies to all CHS staff, the National Team, Board members, Experts by Experience, panel members, Panel Practice Advisors (PPAs), Clerks, and third-party contractors/suppliers with access to CHS systems and/or information.

3.2 CHS is responsible for all information created relating to the Children's Hearings System (the System) by the CHS community (panel members, PPAs, Clerks, CHS National Team, Board Members, Experts by Experience, and third-party contractors/suppliers with access to CHS systems and/or information).

4. Unacceptable Use

4.1 Unacceptable use is:

- Any action which contravenes or potentially contravenes any statutory, regulatory or legislative obligation by which CHS is bound, including data protection legislation, the Human Rights Act 1998 and the Computer Misuse Act 1990.
- Any action which contravenes the policies and procedures laid down by CHS.
- Any action which puts any individual, internal or external to the Hearings System, at risk.

4.2 The activities below are provided as examples of unacceptable use. However, this list is not exhaustive.

- theft or unlawful sharing of IT equipment
- hacking into IT systems
- using illegal or unlicensed software or services on CHS's systems
- contravening copyrights
- violating the privacy of others online
- selling personal data or confidential information
- unlawfully sharing or disclosing personal, sensitive or confidential information outside the organisation
- creating or sending content that is deemed to be offensive, obscene or indecent
- sending or posting discriminatory, harassing, or threatening messages or material which is designed to cause annoyance, anxiety or harm
- introducing malicious software onto CHS's systems
- passing off personal views as representing those of CHS
- corrupting or destroying other user's data
- contravenes CHS's National Standards and values

- Using Children's Hearings email, phones or postal services for non CHS related activity.
- Inputting information about the System or personal data into generative AI tools.

4.3 If you believe that you need to contravene these guidelines in order to perform your role, you must obtain written approval from CHS's Information Governance (IG) team or Senior Information Risk Owner (SIRO) at information@chs.gov.scot before proceeding.

4.4 Contravention of these guidelines may result in temporary removal of access to aspects of CHS's IT systems, permanent removal, and in serious or repeated instances, the National Convener may seek the removal of a Panel Member from the Children's Panel. Staff and Board members may be subject to disciplinary actions.

5. User IDs and passwords

5.1 Maintaining secure access to CHS's systems is critically important, therefore passwords require a minimum of 8 characters and must contain a lower-case letter, an upper-case letter, a number, and a symbol (e.g. !"£$%).

5.2 If you are unable to log in, you should contact the CHS Digital Support Team at digital@chscotland.scot. You can use your personal email to request assistance through this route.

5.3 If you are issued with a temporary password, you must change it as soon as you have logged in successfully as failure to do so presents a serious security risk.

6. Use of email systems

6.1 Clerks, Panel Members, PPAs, Board Members and Experts by Experience must use the provided Children's Hearings email service when sending and receiving any communication relating to the System online. Non-CHS email accounts must never be used to communicate any information relating to the Children's Hearings System or its normal business. Failure to use your CHS account will be considered a breach of this policy.

6.2 Email inboxes must be managed effectively to enable the efficient storage and retrieval of information in line with the CHS Records Management Policy, the Retention & Disposal Schedule, and to support compliance with all relevant legislation.

6.3 You should take care when sending or forwarding emails to ensure that personal, sensitive or confidential data is not being passed on without the appropriate permissions and controls in place. Please check the intended recipient's address carefully before sending an email, as the auto-complete function can result in an incorrect address being selected.

6.4 Emails containing personal data are governed by data protection legislation and must be handled in line with its principles. Personal information includes opinions about an individual or the personal opinions of an individual. Emails containing this type of information must not be disclosed to anyone without the permission of the individual concerned unless there is a clear reason to do so (e.g. to highlight a concern regarding the opinion in line with the Complaints Handling Procedure). If you are not sure on whether to disclose the information, contact the IG Team who will advise accordingly.

6.5 If you accidentally send personal or sensitive personal data to the wrong recipient then you must inform the IG team immediately (email: information@chs.gov.scot) so that the incident is recorded and where necessary to enable CHS to take mitigating actions.

6.6 Children's Hearings email accounts should not be used for personal purposes as an email coming from a Children's Hearings email address is likely to be seen as a communication on behalf of the organisation. Emails sent from your Children's Hearings account will automatically have a disclaimer notice set in to the footer of the email.

6.7 Using a Children's hearings email address provides a secure environment for the transfer of information, which helps us to comply with data protection and information security legislation. However, no system is completely secure and there is still a risk of human error when communicating sensitive information. You should always take extra care when required to share any information that would be classified as OFFICIAL-SENSITIVE[3] (e.g. details which may identify a child, young person or family involved in the System) before sending from/to a Children's Hearings email address. This information must only be shared on a need-to-know basis only. For further guidance, please speak to the IG team.

[3] Please refer to the Security Classifications Policy and Classifying sensitive documents and emails guidance for further information

6.8 Occasionally it may be necessary for CHS to request a user to search their mailbox for information relating to the System. For example, to action:

- Subject Access Requests under data protection legislation
- Freedom of Information requests
- Environmental Information Requests
- Evidence in legal proceedings or a criminal investigation
- An urgent enquiry
- Evidence in support of an investigation into conduct

6.9 Users should carry out a search of their mailbox and forward any relevant information to the CHS National Team when requested. CHS will provide support and guidance to enable you to undertake this.

6.10 If preferred, users may give their permission to a member of the CHS National Team to carry out a search of their Children's Hearings account on their behalf. In these cases, access will be granted to a member of the National Team for a limited period and as soon as the search is complete, the user will be informed that the National Team no longer has access.

6.11 In some cases, it may be necessary, and CHS have the right, to access a mailbox without the permission of the user. For example (but not limited to) when:

- a user leaves the Hearings System and CHS needs to ensure that any vital records are saved in line with CHS's Retention and Disposal Schedule.
- a user is on a leave of absence or does not respond to requests to search their inbox and it is likely there will be vital information or tasks to action within a user's Children's Hearings mailbox.
- a member of the CHS Digital team (including any CHS Digital solutions partners) needs to undertake essential maintenance on a user's Children's Hearings account.
- to recover data sent to an individual's email account in error,
- to assist in incident management,
- for reasons identified in 6.8

6.12 Children's Hearings accounts will be closed on the day a user leaves the system (e.g. last working day or date that a resignation becomes effective). Users must ensure that any vital information has been provided to the Clerk or a member of the National Team to store in line with CHS's Retention and Disposal Schedule prior to their leaving date.

7. Use of personal, mobile and removable devices

7.1 Personal and mobile devices can be remotely connected to CHS systems, but the user is personally responsible for their device and content. These devices are vulnerable, and it is essential that you adhere to the following rules in order to protect the integrity of information and ensure it remains safe and secure:

- devices must have a PIN/password.
- PINs and passwords must be kept confidential and not shared with anyone else.
- You must inform CHS immediately in the event of loss or theft of a device which holds CHS information. CHS can discuss with you and review the CHS information that may be at risk and may wish to exercise the right to take actions to permanently delete this information from the device immediately.
- OFFICIAL-SENSITIVE, confidential and personal data must not be saved/stored on any personal device. It must be accessed and viewed on CHS systems, such as the Community Hub, and must not be downloaded to personal devices.
- Artificial Intelligence (AI) tools must not be used whilst information about the System, sensitive business information, or any information that may directly or indirectly identify any individual is open on your device. CHS-related systems, information and documents must be closed before opening any AI tools on your device.
- Devices and accounts used on the device must not be subscribed to any AI meeting assistants or transcription services.

7.2 Removable devices include, but are not restricted to the following:

- CDs/DVDs
- external hard drives
- USB memory sticks
- media card readers
- embedded microchips (including smart cards and mobile phone SIM cards)
- digital cameras
- audio tapes

7.3 There are several risks associated with the use of removable devices, including the disclosure of sensitive, confidential or personal data as a consequence of loss, theft or careless use; contamination of networks or equipment through the introduction of viruses.

7.4 Removable devices must not be used by the CHS Community, for the storage and transfer of information relating to the Children's Hearings System or its normal business. Information that is to be shared with other members should be made available in the Community Hub or via secure email providing doing so does not breach this Acceptable Use Policy or/and other CHS policies. If there are exceptional circumstances that require the use of removable storage, please contact the IG Team for assistance prior to transferring the data.

7.5 For CHS National Team and Board members, the use of removable devices will be considered on a case-by-case basis. There are substantial risks associated with the use of removable media, and so clear business benefits must be demonstrated before approval is given. Requests for access to, and use of, removable devices must be made to CHS Information Governance & Data Protection Officer (IG&DPO) who will ask users to confirm the reason for using the device. Should access to, and use of, removable media devices be approved the following guidelines may be implemented as appropriate, and once agreed upon must be adhered to at all times:

- devices must be returned to the IG&DPO as soon as use is concluded
- devices must be stored in an appropriately secure place
- all personal, confidential and OFFICIAL-SENSITIVE data stored on removable media, must be encrypted in line with ICO encryption guidance
- virus and malware checking software must be used to scan the device before it is used
- devices that are damaged must not be used, and must be returned for secure disposal
- devices must not be used for archiving or storing records on a long-term basis

8. Use of social media and messaging applications

8.1 Many of us use social networking sites such as Facebook, Instagram, X, YouTube, TikTok and LinkedIn for communicating. They are a quick and cost-effective way of reaching a wide range of people and are a great way for staying in touch and creating communities or promoting the Children's Hearings System. But whilst there are benefits from taking part in social networking, there are things to look out for and think about in your role.

8.2 As partners in the System, we all have a responsibility to uphold its integrity and reputation and to protect the children, young people and families. The guidelines below have been written with a view to allowing the CHS Community to fulfil those responsibilities whilst still enjoying social media.

8.3 When using social media, you should be familiar with the following guidelines:

- The Children's Hearings (Scotland) Act 2011 prohibits the publication of information about any child or young person involved in the System, that is intended, or is likely, to identify them, their address or school. Publication includes newspapers, television, radio and also social networking sites and the internet more generally.

- Web publishing has the same legal status as a written document.

- You must avoid using language that could be seen as defamation, discrimination, abuse, breach of confidence, etc.

- Posting on a social networking site is entirely in the public domain. Information posted online is extremely difficult to remove and may be accessible for a considerable period even after deleted.

- You must not post any personal, confidential or sensitive information relating to the system through social media.

- Social media is often designed to encourage informal communication and sharing of personal views and opinions, so care is needed to ensure that appropriate standards are met, even in a more informal environment. The nature of social media also often leads to a blurring of the distinction between what is public and what is private.

- When using your personal social media accounts (e.g. Facebook, TikTok), you should ensure that any activity on your account is in accordance with your obligations and duties, including CHS's Staff Code of Conduct, the Board Code of Conduct, panel member code of conduct, the National Standards for the Children's Panel and ASTs: Functions, Roles and Responsibilities. It is your personal responsibility to ensure that social media activity in your name does not breach these requirements or bring the Children's Hearings System or CHS into disrepute.

- Linking to (e.g. following/being friends with) other people involved in the System e.g. Children's Reporters, Safeguarders, social workers must be avoided. Care must be taken to avoid inappropriate and unlawful online communication, such as discussing a case or posting any other confidential information, and any potential or perceived conflict of interest. Even 'direct messaging' (private communication between two individuals) is not necessarily secure. Issues such as conflict of interest may also arise, with the possibility that a perception of conflict may be created even if the individual does not consider a conflict to exist.

- Social media must not be used to communicate any operational information provided to you to carry out your role within the System, even if this is done in private or closed groups with other individuals involved in the System.

- You must never link with or befriend any children, young people or families within the system who you have met through your role in the System. If you are contacted by a child, young person or family member via a social networking site, please inform your local AST.

- Posting chain letters, promoting or condemning causes/beliefs, or posting abusive or offensive materials should be avoided as it may cause offence or breach the National Standards.

- As a partner in the System any comments made regarding the operation of the System, discussions about panel members and PPAs, actual hearings/cases, social work, SCRA, CHS etc. could easily be misused and must be avoided. If you feel compelled to express a view or respond to a query on the System, you should make it explicitly clear that the views expressed are your own and not made on behalf of CHS.

- Some social media sites invite you to publicly state your place of work or volunteer role. If you choose to do this, you should be aware that opinions which you express are more likely to be linked with your role within the System and extra care should be taken to follow the above guidelines.

8.4 If you see something on social media that you believe to constitute a breach of this policy and/or the Children's Hearings Act (2011), please contact communications@chs.gov.scot

8.5 WhatsApp and other messaging applications must not be used for CHS business unless these have been pre-approved by the Information Governance team. Microsoft Teams and email using your CHS account must always be used for CHS business and communications related to your role at CHS.

9. Use of Microsoft Teams

9.1 You will have the opportunity to have your say on news items, articles, blogs and discussion forums within Microsoft Teams. Comments are welcomed as they make Teams more interactive and interesting. CHS moderates comments as CHS expects all users to comply with this policy and to be respectful of all other users of the system. CHS reserves the right to remove any comments or close down any discussion forums which do not comply with this policy.

9.2 Some Teams and Channels will be organisation-wide, which means they are open to everyone, while some Teams and Channels will be restricted, for example local area teams are open only to those in the local area.

9.3 No matter what Team, Channel or chat you are in, you must abide by this policy, and the guidance set out below. Failure to do so will be considered a breach of this policy.

9.4 Before you post any comments, please consider the following:

- your name will be posted automatically - no posts can be made anonymously.
- Do not say anything online that you would not say in person.
- do not use channels or chats to complain about issues which should be addressed via your regional team/line manager or the official complaints procedure - some topics will undoubtedly arouse strong emotion, so please consider your comment before posting it.

- Ensure your comments are appropriate, relevant, and:
    - do not provoke or offend others.
    - Do not identify any child, family or specific case details.
    - are not racist, sexist, homophobic, abusive or otherwise objectionable.
    - do not contain language or a tone that are likely to offend others.
    - are not considered an attack on others, including panel members, PPAs, Clerks, CHS National Team, Experts by Experience and Board members.
    - do not break the law, such as potentially libellous or defamatory postings, or those in potential breach of copyright.
    - are accurate and not likely to mislead others.
    - respect other people's opinions and are courteous to all other users

- Local/Regional teams will only be open to members of that area, panel members sitting on hearings within that area, local clerks and certain CHS National Team members (such as the Tribunal Delivery Manager). Local area Teams will be moderated by Regional Teams and Clerks. Part of their role will be to monitor discussions and postings and report to the Digital Team who will close any inappropriate dialogue or threads.

- CHS National Team forums will only be open to staff and Board members and will be moderated by a member of staff.

- National community discussion forums will be open to all users of Children's Hearings Scotland and will be moderated by the Communications Team. Moderators will monitor discussions and postings and close down any inappropriate dialogue or threads.

- It is your responsibility to ensure your comments meet these guidelines and to show consideration for others.

- Comments which are considered by a moderator not to meet the above criteria may be passed to the Tribunal Delivery Manager/your line manager for information.

9.5 If you find a comment offensive you should contact your Tribunal Delivery Manager/line manager outlining your concerns.

9.6 If you post comments which are deemed to contravene this policy, they will be removed, and you will be asked to refrain from making similar statements. If this happens three times in a twelve-month period, you will be removed from Teams for a period of three months.

9.7 Teams Telephony will be accessible to selected staff members for handling incoming calls from the general public and panel members. These calls are intended to provide support to the Panel Member community and to address various queries from young people and the general public. If you have access to this service, please ensure that all outgoing calls are strictly business-related and made in the fulfilment of official CHS duties.

10. Use of OneDrive

10.1 Microsoft Teams uses the Microsoft Office 365 platform which provides users with access to Microsoft's cloud storage, OneDrive. OneDrive also provides users with greater functionality in Teams, to share and collaborate on documents. The use of OneDrive has many benefits, but there are also additional risks.

10.2 OneDrive is only authorised for the temporary storage of non-sensitive information for CHS business purposes.

10.3 OneDrive must not be used for long term storage of OFFICIAL-Sensitive information (e.g. information relating to a hearing), commercially sensitive information, or for any non-CHS related business.

10.4 Each user is personally responsible for ensuring that the information kept on their OneDrive is kept no longer than is necessary and only held for the purposes for which it was obtained. All information should be either deleted or moved to an approved storage location (e.g. the National Team G: Drive on SCOTS).

10.5 A sharing function is available on OneDrive which allows users to share a document directly with other users. Any information stored on your OneDrive should be set to "only you". If you wish to share information electronically, please ensure that doing so does not breach this Policy.

10.6 The Community Hub provides a range of options for the storage and communication of information, including CSAS and CHS email. OneDrive is not intended and should not be used to replace these functions. Inappropriate use of OneDrive constitutes a breach of this Policy.

11. Use of IT and Communications Equipment

IT and communications equipment, including laptops and mobile phones, may be provided to you in order to support you in your role. If CHS provides you with equipment, you must follow the guidelines below:

- It must only be used for the purpose of carrying out your role, personal use of CHS provided equipment is not permitted.
- It must only be used by the registered PPA, panel member, CHS National Team or Board member and must not be passed on to anyone else for use
- It must be always kept in a safe place
- if equipment provided to you by CHS is lost or stolen, you must report this to CHS immediately to the IG team at information@chs.gov.scot
- if equipment provided to you by CHS is faulty, you must contact CHS to arrange for its collection and return
- on leaving CHS, you must ensure that all equipment is returned to CHS
- Passwords must meet the requirements described in Section 5 of this Policy
- Passwords must be kept confidential
- devices should automatically activate their password after 5 minutes of inactivity

- You must inform CHS immediately in the event of loss or theft of a device which holds CHS information (please see the Data Protection Policy and Managing Information Security Incidents Procedure for further information)

- Children's Hearings email may only be accessed on mobile devices using the Microsoft Application outlined within this policy

- OFFICIAL-SENSITIVE, confidential and personal data must not be saved/stored on any mobile personal device. Except for the use of Microsoft Applications as outlined in this policy.

- Work mobiles and Teams telephony should only be used to make business related calls

- Artificial Intelligence (AI) tools must not be used whilst information about the System, sensitive business information, or any information that may directly or indirectly identify any individual is open on a device. CHS-related systems, information and documents must be closed before opening any AI tools on a device.

12. Use of the internet

12.1 CHS National Team and Board members should refer to the SG IT Code of Conduct for guidance on the acceptable use of the internet when using SCOTS computers and SCOTS Wi-Fi.

12.2 Anyone using CHS's internet/Wi-Fi network at Thistle House must ensure that their use of the internet complies with this policy.

13. Breach of this policy

13.1 All users have a responsibility to adhere to this policy. If a user is found to have used CHS's IT facilities or information in a way that would be deemed unacceptable, access may be suspended, pending an investigation. Repeated breaches may result in access to certain services being removed or reduced, and in serious cases, removal from the System. For CHS National Team members, a serious breach of this policy may lead to disciplinary action and dismissal, in accordance with the Staff Code of Conduct. A serious breach of the policy by a Board member may lead to investigation by The Standards Commission for Scotland in line with the Board member's Code of Conduct. Breaches of this policy by a panel member or PPA may result in the member being removed. Breaches of this policy by an Expert by Experience may result in removal from their role at CHS. Breaches of this policy by a Clerk, a member of their team, or a third-party contractor/supplier with access to CHS systems/information may result in termination of CHS' contract with the third-party.

13.2 Any investigation of misuse will be facilitated by this policy.

13.3 Further to this, the Computer Misuse Act 1990 identifies three criminal offences of computer misuse, including unauthorised access to computer material, unauthorised access with intent to commit or facilitate further offences and unauthorised modification of computer material. Penalties for breaches of this Act can be severe, ranging from a fine to five years in prison. It is important that users understand that a breach of this policy and this Act may lead to a criminal investigation and they will be personally liable for any fines or penalties imposed, as a result of the breach.

13.4 Users should report any suspected or known breaches of this policy to CHS immediately. Please refer to CHS's Managing Information Security Incidents Procedure (CHS National Team, Clerks, and Board members) or Reporting information security incidents (summary guidance for volunteers) for further information.

13.5 In using CHS's IT facilities and services each user agrees that CHS shall have no liability for the loss or damage to any user-owned equipment, devices, systems or other assets resulting from the inappropriate use or misuse of the IT infrastructure.

14. Monitoring and review

14.1 CHS will monitor the use of its IT systems and the information held on its systems, on a regular basis. Compliance with this policy will be monitored by CHS's Senior Information Risk Owner (SIRO) and regular audits of networks and systems will be undertaken. CHS acknowledge that it will be necessary to play a proactive part in identifying, monitoring and managing risks to information as new ways of accessing and using information are developed in the future. The policy will be reviewed every year in order to take account of any new or changed legislation, regulations or business practices, or use of new technology.

15. Implementation, Communication and Compliance

15.1 To implement this policy, all volunteers and staff are required to read this policy as part of their mandatory Information Governance training, and the most up-to-date version is available and accessible on the CHS website.