children's hearings scotland

The Children's Panel – life changing.

Acceptable Use Policy

1. Introduction and purpose

1.1 CHS is responsible for all information created relating to the Children's Hearings System (the System) by the CHS community (panel and AST members, Clerks to the AST, CHS National Team and Board Members). This includes all information generated using any CHS systems, e.g. Children's Hearings Information and Resource Portal (CHIRP) which is provided on the Microsoft Office 365 platform and includes all systems included in the Office 365 offering provided now and in the future and Rota Management and Training records applications, provided for in the Childrens Hearings Service Panel Pal system. 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.

1.2 This *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. It defines the ways in which CHS' online systems must be used, 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[1].

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

1.4 For the purposes of this policy, 'users' relates to panel and AST members, Clerks to the AST, CHS National Team and Board members. 'Systems' relates to CHIRP (including email) and Panel Pal. References to the word 'device' relates to all IT equipment (except SCOTS equipment) used to gain access to CHS systems (including but not limited to: mobile phones, laptops, desktop computers, iPads and tablets.).

1.5 All information held within CHIRP and Panel Pal has been provided to support you in your role. This information should not be shared with anyone outside of the organisation without authorisation. This includes sharing electronically (soft copy), printed copies, information on social networking sites, publication online, verbally and printed media.

[1] 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).

Date Approved: 11/05/2018
Date for Review: 11/05/2020

2. Unacceptable use

2.1 Unacceptable use is defined by CHS as any action which contravenes or potentially contravenes any statutory, regulatory or legislative obligation by which CHS is bound, including the data protection law and other information legislation, the Human Rights Act 1998 and the Computer Misuse Act 1990. It is also any action which contravenes the policies and procedures laid down by CHS.

2.2 Unacceptable use can also be defined as any action which puts any individual, including a child, young person or family, a panel or AST member, member of CHS National Team or Board, at risk. The activities below are provided as examples of unacceptable use; however this list is not exhaustive. Should you need to contravene these guidelines in order to perform your role, you should obtain approval from CHS' Information Governance (IG) team or Senior Information Risk Owner (SIRO) before proceeding. Examples of unacceptable use include but are not limited to:

- *theft of IT equipment*
- *hacking into IT systems*
- *contravening copyrights and patents*
- *procuring or selling personal data*
- *using illegal or unlicensed software or services on CHS systems*
- *breaching data protection legislation*
- *sharing or disclosing sensitive 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 images*
- *introducing malicious software onto CHS systems*
- *sending or posting chain letters or advertisements not related to CHS purposes or activities, or on behalf of CHS without its knowledge*
- *passing off personal views as representing those of CHS*
- *creating or sending material which is designed to cause annoyance or anxiety*
- *corrupting or destroying other user's data*
- *violating the privacy of others online*
- *contravenes CHS' National Standards and values*
- *Using CHIRP email for non CHS related activity (refer to Section 4.6)*
- *Using CHIRP email to send information that would be classed as OFFICIAL – SENSITIVE (Appendix I)*

3. User IDs and passwords

3.1 The use of another individual's User ID and password is not permitted under any circumstances. You must not disclose your passwords and must take all reasonable precautions to ensure that your password remains confidential. If you disclose your password to someone else you may be held responsible for any improper actions committed under that User ID and accountability may fall equally on you as the holder of the account, as on the individual using the account at the time.

3.2 Maintaining secure access to CHS systems is critically important, therefore CHIRP passwords require a minimum of 8 characters and must contain:

A lower case letter
An uppercase letter
A number
A symbol (e.g. !%&*)

Passwords will expire after 180 days and you will be required to select a new password. When selecting a new password, previous passwords will not be allowed. If you cannot remember your password, you can use the "Forgotten my password" link to reset the password. This will send a password reset email to the personal email address that you provided when you signed up for CHS systems, e.g. CHIRP The e mail will then enable you to create a new secure password.

3.3 If you enter the wrong password 10 times, you will be required to complete a CAPTCHA test to continue. This is an online test that enables a computer to confirm you are human and not a computer that is trying to hack into the account. It will most likely present a series of letters or pictures and ask you to re-type the word or select the relevant pictures from a set. If you fail to login a further 10 times, you will need to contact our IT Helpdesk on 0333 456 4770; or email CHSITSupport@Imassist.com, to reset it. You can use your personal email to request assistance through this route. 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.

4. Use of email systems

4.1 Panel and AST members must use CHIRP email service when sending and receiving any communication relating to the System online. Operating this way is the simplest and safest way to ensure that privacy issues do not arise. Personal (or non-CHIRP) email accounts must never be used to communicate any information relating to the Childrens Hearings Service or its normal business. Continued use of personal email accounts to communicate this information will be considered a conduct issue and may lead to removal as a panel or AST member.

4.2 Email must be managed effectively in order to enable the efficient storage and retrieval of information and in line with CHS Records Retention Policy; and support compliance with all relevant legislation, including the Data Protection legislation, Freedom of Information (Scotland) Act 2002 and Public Records (Scotland) Act 2011.

4.3 You should take care when sending or forwarding emails in order to ensure that personal, sensitive or confidential data is not being passed on without the appropriate permissions and controls in place. In particular, 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. Or alternatively you can switch off the auto-complete function by entering:

Outlook > File > Options > Mail > Send Messages then un-tick the box "use auto complete list to suggest names when typing in the To, CC & BCC lines" and un-tick the box "automatic name checking".

4.4 Emails containing personal data are covered by data protection legislation including the General Data Protection Regulations 2016 (GDPR) and Privacy and Electronic Communications Regulations (PECR) and must be handled in line with its principles. Under this suite of legislation , personal information is defined and the definition 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 CHS Community Concerns Procedure). If you are not sure on whether to disclose the information, contact the IG Team who will advise accordingly.

4.5 If you accidentally send personal or sensitive personal data to the wrong recipient then you must inform the IG team immediately (email: information@chs.gsi.gov.uk) so that the incident is recorded and where necessary to enable CHS to report to the UK Information Commissioner's Office (ICO) within the 72 hour response time requirement.

4.6 CHIRP email accounts should not be used for personal purposes as an email coming from a Children's Hearings email address is likely to be perceived as a communication from someone acting on behalf of the organisation. E mails sent from your CHIRP account will automatically have a disclaimer notice set in to the footer of the e mail. Personal email accounts should always be used to send personal emails.

4.7 Using a CHIRP email address provides a secure environment for the transfer of information which helps comply with data protection legislation as well as other information governance legislation. However, no system is completely secure and there is still a risk of human error when communicating sensitive information so you should always redact any information that would be classified as OFFICIAL-SENSITIVE[2] (e.g. details which may identify a child, young person or family involved in the System) before sending from/to a CHIRP email address. This information must be shared on a need to know basis only. If it is absolutely necessary to share the name of a child, young person or family member in order to deal with a particular issue, e.g. a complaint, then this should be shared over the phone (but not left as a voice message) and only the time, date and location of a hearing should be recorded in electronic communications and records. For further guidance, please speak to the IG team.

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

4.8 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

4.9 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.

4.10 If preferred, users may give their permission to a member of the CHS National Team to carry out a search of their CHIRP 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.

4.11 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 System and CHS needs to ensure that any vital records are saved in line with CHS' 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 CHIRP mailbox
- a member of the CHS IT team (including any CHS IT solutions partners) needs to undertake essential maintenance on a user's CHIRP account
- to recover data sent to an individual's email account in error, to assist in incident management
- For reasons identified in 4.8

4.13 CHIRP 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 should ensure that any vital information has been provided to the Clerk or a member of the National Team to store in line with CHS' Retention and Disposal Schedule prior to their leaving date.

5. Use of OneDrive

5.1 CHIRP uses the Microsoft Office 365 platform which provides users with access to Microsoft's cloud storage, OneDrive. Cloud storage can allow users to access saved documents by logging in from any internet connected device. The use of cloud storage has many benefits but there are also additional risks.

5.2 OneDrive in CHIRP is the only authorized cloud storage system, for the purposes of temporary storage of non-sensitive information for CHS business.

5.3 OneDrive in CHIRP must not be used by CHIRP users for the storage of OFFICIAL-Sensitive information (i.e. special categories of personal data as defined in CHS' Data Protection Policy or commercially sensitive information).

5.4 Each user is personally responsible for ensuring that information is not kept on their CHIRP OneDrive for longer than is necessary and only held for the purpose by which it was obtained for. All information should either be deleted or transferred to a CHS approved storage location (e.g. a Clerk's Office or the National Team's drives on SCOTS).

5.5 A sharing function is available on OneDrive which allows users to share a document directly with other users. CHS believes that the risks of sharing information in this way outweigh the benefits. Any information stored on your CHIRP OneDrive should be set to "only you". If you wish to share information electronically, please check with CHS IG team regarding the best way of achieving your need regardless it will be based on the principle that doing so does not breach this Acceptable Use Policy.

6. Use of personal, mobile and removable devices

6.1 Personal and mobile devices can be remotely connected to CHS systems, but the user is personally liable for their device and content. These devices are especially vulnerable and so 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 be locked with a PIN/password
- PINs should be at least 4 digits long and passwords should match the requirements of those for CHIRP as described in Section 3.
- PINs and passwords must be kept confidential and not shared with anyone else
- devices should automatically activate their PIN/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. 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[3]

[3] Please see *Data Protection Policy* and *Managing Information Security Incidents Procedure* for further information.

- CHIRP email can be accessed on mobile devices using the Microsoft Outlook application. . If you download the application to your device and set it up for CHIRP e mail you will initially receive a message stating this action is quarantined. This is OK, it is because CHS need to authorise your account to access the application. The application will automatically send a request for authorisation to the CHS IT Team who will normally authorise your account within 48 hours (Monday – Friday). For Download instructions please refer to Microsoft Outlook Application Instructions in the IT portal in CHIRP.
- It is a requirement of use that you adhere to this Acceptable Use Policy.
- OFFICIAL-SENSITIVE, confidential and personal data must not be saved/stored on any mobile personal device outwith use of the Microsoft Application outlined within Appendix II of this policy.

6.2 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

6.3 There are a number of 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. These may result in potential sanctions against CHS or individuals imposed by the UK Information Commissioner's Office (ICO); potential legal action against CHS or individuals; and potential reputational and financial damage.

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

6.5 For CHS National Team and Board members, the use of removable devices will only be approved if a valid business case for its use is developed. 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 IG Lead 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 must be adhered to at all times:

- devices must be returned to the IGLead 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

- damaged or faulty devices must not be used
- virus and malware checking software must be used
- devices that are damaged must be returned for secure disposal
- only devices purchased and installed by CHS may be used to connect to CHS' IT systems
- devices must not be used for archiving or storing records on a long term basis

7. Use of social media

7.1 Many of us use social networking sites such as Facebook, Instagram, Twitter, YouTube and Linked-In for communicating. They are a quick and cost effective way of reaching a wide range of people and are 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.

7.2 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 panel and AST members, Clerks, CHS National Team and Board members to fulfil those responsibilities whilst still enjoying social media.

7.3 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 should 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 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, Twitter), you should ensure that any activity on your account is in accordance with your obligations and duties, including CHS' Staff Code of Conduct, the Board Code of Conduct, panel member terms of appointment, 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 should be treated with common sense. 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. It is worth remembering that 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 should 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. Only CHIRP email should be used for online communication of operational information regarding the System providing doing so does not breach this Acceptable Use Policy..

- 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 or the Panel and Area Support Team at CHS.

- 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 and AST members, actual hearings/cases, social work, SCRA, CHS etc. could easily be misused and should 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. Use of discussion forums

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

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

- your name and role will be posted automatically - no posts can be made anonymously
- please don't say anything online that you wouldn't say in person
- please ensure your comments:
  - are appropriate and relevant - please don't use forums and blogs to complain about issues which should be addressed via your AST/line manager or the official complaints procedure - some topics will undoubtedly arouse strong emotion, so please consider your comment before posting it
  - do not provoke or offend others
  - 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 and AST members, CHS National Team 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

- AST discussion forums will only be open to members of that AST, panel members sitting on hearings within that AST area and CHS National Team members. AST discussion forums will be moderated by a member of the AST. Moderators will monitor discussions and postings and close down any inappropriate dialogue or threads.

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

- National discussion forums will be open to all users of CHIRP and will be moderated by a member of the CHS National 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 Area Convener/your line manager for information.

8.3 If you find a comment offensive you should contact your Area Convener/line manager outlining your concerns. If you think a comment is wrong or inaccurate you should contact the individual directly or post up a factual correction.

9. Use of IT and communications equipment

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

- *equipment must only be used for the purpose of carrying out your role, personal use of CHS provided equipment is not permitted;*
- *equipment must only be used by the registered AST or panel member, CHS National Team or Board member and must not be passed on to anyone else for use;*
- *equipment must be kept in a safe place at all times;*
- *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.gsi.gov.uk*
- *if equipment provided to you by CHS is faulty, you must contact CHS to arrange for its collection and return;*
- *on leaving the System/CHS, you must ensure that all equipment is returned to CHS.*devices must be locked with a PIN/password
- PINs should be at least 4 digits long and passwords should match the requirements of those for CHIRP as described in Section 3.
- PINs and passwords must be kept confidential and not shared with anyone else
- devices should automatically activate their PIN/password after 5 minutes of inactivity
- You must inform CHS in the event of loss or theft of a device which holds CHS information immediately[4]
- CHIRP e mail 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 outwith use of the Microsoft Application outlined within this policy.

10. Use of the internet

10.1 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 WiFi

10.2 Anyone using CHS' internet/WiFi network at Ladywell House must ensure that their use of the internet complies with this policy.

[4] Please see *Data Protection Policy* and *Managing Information Security Incidents Procedure* for further information.

11. Breach of this policy

11.1 All users have a responsibility to adhere to this policy. If a user is found to have used CHS' IT facilities or information in a way that would be deemed unacceptable, access may be suspended, pending an investigation. 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 or AST member may result in the member being removed.

11.2 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.

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

11.4 In using CHS' IT facilities and services each user agrees that CHS shall have no liability for the loss or corruption of any user file or files, information or data; and/or 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.

12. Monitoring and review

12.1 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' 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 two years in order to take account of any new or changed legislation, regulations or business practices, or use of new technology.

Document Control

Title	Acceptable Use Policy
Author	Ava Wieclawska
Approved by	CEO
Date of approval	March 2018
Version number	8.0
Review frequency	Every two years
Next review date	March 2020

Status Control

Version	Date	Status	Author(s)	Amendments to policy	Approved by
1.0	18/06/2013	Final	Ava Wieclawska and Lesley Taylor	N/A	SMT
2.0	05/09/2013	Final	Ava Wieclawska	Removal of reference to posting humorous comments at 7.3.	SMT
2.1	20/02/2014	Draft	Ava Wieclawska	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.	SMT
2.2	02/06/2014	Draft	Ava Wieclawska	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.	
2.3	19/08/2014	Draft	Ava Wieclawska	Policy reviewed by Audit and Risk Management Committee (ARMC) – no changes recommended.	ARMC
3.0	26/08/2014	Final	Ava Wieclawska	Final policy approved by the CHS Board.	CHS Board
3.1	25/03/2015	Draft	Ava Wieclawska	Minor amendments to section 4.6 and to reflect revised job titles	SMT
4.0	31/03/2015	Final	Ava Wieclawska	Final policy approved by SMT	SMT
4.1	11/05/2015	Draft	Ava Wieclawska	Removal of section 4.8	SMT
6.0	11/05/2015	Final	Ava Wieclawska	Final policy approved by SMT	SMT
6.1	29/06/2016	Draft	Callum Morrison	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.	
6.2	July 2016	Draft	Ava Wieclawska	Minor amendments to terminology	

6.3	October 2016	Draft	Callum Morrison	Amendments to terminology and social media guidance in line with CEO comments	
7.0	05/01/2017	Final	Alice Wilson and Callum Morrison	Final Policy Approved by CEO	CEO
7.1	31/08/2017	Draft	Callum Morrison	Changes made to terminology for GDPR and minor updates to procedure.	
7.2	22/01/2018	Draft	Ellie Robertson	Changes made to terminology for GDPR and minor updates to procedures & Panel Pal	
7.3	20/02/2018	Draft	Alice Wilson	Further checks for GDPR, prior to sending to SMT to approve.	
8.0	22/03/2018	Final	Alice Wilson	Approval of revisions	SIRO
9.0	09/05/18	DRAFT	Lynne Harrison	Amendments to enable Outlook App mobile access to CHIRP	
10.0	11/05/2018	Final	Lynne Harrison	Final Policy Approved	SIRO

Appendix I

Examples of OFFICIAL-SENSITIVE information

All information created by panel and AST members and Clerks is classed as OFFICIAL. Information which contains the following would be classed as OFFICIAL – SENSITIVE

The **sensitive personal data** of an individual, including information relating to their:

racial or ethnic origin
political opinions
religious beliefs or other beliefs of a similar nature
membership of a trade union
processing of genetic data
biometric testing
physical or mental health or condition
sexual life
commission or alleged commission of any offence
court proceedings for any offence committed or alleged to have been committed by the individual

CHIRP email accounts provide a secure platform for the transfer of information, however, no system is entirely secure and there is always a risk of human error. As such OFFICIAL-SENSITIVE information should not be communicated via CHIRP email unless it is **absolutely necessary** and has had prior approval from CHS' Information Governance (IG) team or Senior Information Risk Owner (SIRO).

Wherever possible, information which is considered OFFICIAL-SENSITIVE should be redacted to remove sensitive information before being sent via email (e.g. details which may identify a child, young person or family involved in the System).

If you need to share the name of a child, young person or family in order to deal with a particular issue, e.g. a complaint, then this should be shared over the phone and only the time, date and location of hearing should be recorded in electronic communications and records.