Keeping information safe - key tips for Clerks

Information relating to the Children's Hearings System is confidential & must not be disclosed to anyone outside of the System. To ensure that this information is kept safe at all times, Clerks & their teams must follow the guidelines below in line with the MOU between your local authority & CHS:

- ✓ keep confidential & personal information relating to the System locked away in pedestals/cabinets when not in use or in a secure electronic system, with access available only to authorised staff ensuring all devices used to access CHS IT systems are protected with a strong PIN/password
- ✓ dispose of all confidential paper waste either using the local authority's approved shredding contractor or using an onsite cross-cut shredder
- ✓ inform the CHS IG team immediately at information@chs.gsi.gov.uk (but no later than 12 hours from the time you became aware of the incident), if you think that information has been lost, stolen, destroyed, damaged or disclosed to someone who is not authorised to have it (in paper, electronic, sound, visual or audio format). Emergencies should be reported to the IG Lead by mobile telephone
- ✓ when sending emails or taking telephone calls, double check that you have the correct recipient(s) before sending or forwarding confidential or personal information
- ✓ keep information relating to the System separate from local authority information on electronic systems & keep it up to date & accurate
- ✓ use a secure GSI/CHIRP email account when sending emails relating to the Hearings System
- ✓ Pass all requests for information (i.e. FOI, EIR & SAR) & complaints to CHS immediately (but no later than 2 working days) to information@chs.gsi.gov.uk & complaints@chs.gsi.gov.uk respectively

- ✘ do not comment on or share any confidential or personal information on social media
- ✘ do not access confidential or personal information in public places
- ✘ do not leave personal or confidential information unattended at any time – this includes information on a computer screen & information on paper documents
- ✘ do not use or share personal details of AST & panel members without their explicit consent
- ✘ do not store or transfer out with the EEA any personal or confidential information on removable devices (including memory sticks/CDs/unencrypted laptops) or keep data for longer than necessary, adhering to retention rules & schedule 2 of the MOU specifically sensitive personal data, PVG, recruitment, resignations, finance, bank details, training & details on rotas
- ✘ do not share your password details with anyone else
- ✘ do not send any information relating to the System to/from personal email accounts