

# Sharing sensitive and confidential information electronically - Important information for staff

All employees are under a legal obligation under the DATA PROTECTION ACT 1984 not to use or disclose any personal information that comes into their possession in the course of their duties in any unauthorised manner. Duties and obligations under the Act that relate to a particular post will be explained to the post holder upon appointment to the post.

## Do

- send identifiable, confidential and/or sensitive data on children, young people, staff or other persons only in limited and controlled circumstances and using a secure method of interagency communication.
- keep a record of any regular and ad-hoc transfers sent outside of the authority. A proforma is available in the full guidance.
- remove any confidential or personal details from external emails received (e.g. from a member of the public) before replying to the sender so as to minimise the degree of identifiable information used in correspondence.
- keep sensitive data to a minimum and never include identifiable personal details in the subject line of an email.

## Don't

- send or transport unencrypted and unprotected sensitive and/or confidential information on memory stick, CD/DVD/floppy disk/removable hard disk or a laptop.
- include identifying details of individuals in emails or documents unless absolutely necessary.
- forward emails containing confidential or sensitive information outside of the authority inadvertently or without suitable encryption.

## What isn't secure

- e-mails sent from a *southglos.gov.uk* email account to any non southglos.gov.uk address are NOT secure as the information passes over the internet unencrypted. This also includes emails sent to schools with non southglos email addresses (e.g. Secondary Schools, Pupil Referral Unit, our colleagues in health, police, fire and rescue)

## What is secure

- secure email accounts\* should be used to transfer sensitive information to other agencies. If this is not possible then encryption methods such as RM SecureNet Plus, NHS SecureSend<sup>†</sup> or WinZip must be used to protect information and data (see [E-mail supplementary guidance](#) ref D410-1-016-10).

---

\* secure e-mail account transfers include those emails sent and received between a \*.gcsx.gov.uk, \*.police.uk, \*.pnn.police.uk, \*.scn.gov.uk, \*.cjsm.net, \*.nhs.net domain account. Once \*.gcsx.gov.uk accounts are available to staff, this will be the preferred solution for sending and receiving sensitive and confidential data and information between organisations that also have a secure email domain as above

<sup>†</sup> Further information on SecureSend available in full guidance document "[Email Operational Guidance](#)"