

## SNAs

Everyone within the School has a role to play in ensuring that the School can “demonstrate compliance” with data protection laws. Set out below are some examples of the ways each person within the School community can help. These lists are by no means exhaustive; each School should consider how each of its key players can help uphold privacy, ensure ethical information governance, and respect data protection



Adhere to information governance protocols if making changes (deletions, additions etc).



Adherence to high standards of ethics and professionalism in all data entries



Ensure that any handwritten notes in any notebook are transferred to the school administrative system as soon as possible (to ensure availability of data, allowing appropriate back-ups to be made, accountability, transparency, keeping data safe and secure, etc).



Use strong passwords (12 characters, mixture of alphanumeric, upper- and lower-case, and symbols) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!).

---

## SNAs



Take responsibility for keeping sensitive data-sets safe and secure

---



Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts etc).

---



Never sharing work-related data on unapproved systems (e.g. talking about a student in a WhatsApp group).

---