

## ENCRYPTED MEMORY STICK/MOBILE PHONE STAFF AGREEMENT

I understand that use of a memory stick is only permitted where the memory stick is encrypted, and all data saved on it is encrypted with a strong password. I will abide by the Astrea Academy Trust Data Protection policy to only use Encrypted memory sticks when handling Astrea Academy Trust personal data.

I understand that if I have access to Astrea emails via a mobile phone (Personal or Trust provided device) that mobile phones are password protected and where applicable, emails accessed via the Outlook App.

### Important:

- I confirm that I have backed up/deleted all sensitive data relating to pupils and staff from my existing, unencrypted, memory sticks and removable drives
- I confirm that backed up personally identifiable data is held in a secure location (password protected) on a work device and not a home device -
- I confirm I have checked my home device and I do not hold any historical personal data relating to pupils or staff
- I understand that I must abide by this code of conduct and non-compliance could lead to disciplinary procedures.
- I understand that any loss of data (electronic or paper copies) must be reported as a breach immediately. Report to the School Business Manager/Principal who will refer to the Trust DPO. If required Astrea DPO will notify the ICO. Note: deadline for reporting to the ICO is 72 hours from finding the breach, not reporting it. – **TIME CRITICAL**
- I confirm that mobile phones used to access Astrea Academy Trust email account are password protected and where applicable, emails accessed via the Outlook App.

**Please indicate your understanding and acceptance of the above by entering a tick into the box on**

**Athena Policies and Procedures**