**GDPR E-Security Policy**

**Strategic and operational practices**

At this school:

* The Head Teacher is the Senior Information Risk Officer (SIRO).
* Nicola Cook is the Data Protection Officer (Schools DPO Ltd) with responsibility for data protection compliance.
* Staff are clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners.
* Cortec report any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
* All staff are DBS checked and records are held in one central record under Single Central Record on SEN Drive.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement. We have a system so we know who has signed.

* staff
* pupils
* parents

This makes clear all responsibilities and expectations with regard to data security.

* We have approved educational web filtering (Eset) across our wired and wireless networks.   
  We also have <an additional layer of monitoring software across our network system>.  
  We monitor school <e-mails / blogs / online platforms, etc.> to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.
* We follow The Tutorial Foundation guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
* All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
* We require staff to use STRONG passwords for access into Office 365 system.
* We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. All information is held on 365.
* School staff who set up usernames and passwords for e-mail, network access, work within the approved system and follow the security processes required by those systems.
* We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored. This is covered in our Acceptable Use Policy.

**Technical or manual solutions**

* Staff have secure area(s) on the network to store sensitive documents or photographs.
* We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 mins. idle time. This is part of our Acceptable Use Policy.
* Staff do not use USBs.
* We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
* We use Office 365 for online document storage.
* We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area.
* All servers are in lockable locations and managed by DBS-checked staff.
* We comply with the WEEE directive on equipment disposal: Cortec is responsible for the disposal of IT equipment.
* Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
* Paper based sensitive information is shredded, using a cross-cut shredder.

|  |  |
| --- | --- |
| **Policy review date** | **December 2022** |
| **Date of next review** | **December 2023** |
| **Who reviewed this policy?** | **Julia Low, Headteacher** |