eSafety and Data Security Policy

Updated January 2017
Review Date: January 2018

This is a summary of Adeyfield School's eSafety and Data Security Policy. The full policy can be requested from the Headteacher's PA.

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Karen Howard who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as HCC, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

- At this school we have an Acceptable Use policy which all staff sign. Copies are kept on file.
- ICT Acceptable Use Agreements are signed by all Staff/Students.
- All members of the school who have access to sensitive or personal data are given training on the importance of this data.

Protected and restricted material must be encrypted if the material is to be removed from the school.

- At this school we use the DfE S2S site to securely transfer CTF student data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer, using the DfE secure export to Local Authority Student Database.

Sensitive or personal material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At this school we store such material in lockable storage cabinets in a lockable storage area.
- At this school all servers are in lockable locations and managed by DBS-checked staff.
- At this school we use follow LA back-up procedures and lock the tapes in a secure cabinet.

Disposal: Sensitive or personal material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At this school we use the Prm Green Technologies for disposal of system hard drives where any protected or restricted data has been held. All server hard drives are physically destroyed.
- At this school paper based sensitive information is shredded, using cross cut shredders.
- Laptops used by staff at home (loaned by the school) where used for any protected data are brought in and disposed of through the same procedures.
- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems eg for email, network access, SLG and Learning Platform access are supported by the LA ICT Support Service.
- Security policies are reviewed and staff updated at least annually and staff know to whom they should report any incidents where data protection may have been compromised.