Malden Oaks
Investing in success

Dukes Centre
Dukes Avenue
Kingston KT2 5QY

020 8547 6711
020 8547 6660

E-safety policy

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- 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 in a spreadsheet.
- We ensure staff know to immediately report, and who to report to, 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.

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

  - staff
  - students
  - MC members

  This makes clear all responsibilities and expectations with regard to data security.
- We have approved educational web filtering across our wired and wireless networks. We also have monitoring of school e-mails / blogs / learning platforms, etc
- We follow LA 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 our MIS system and that these are changed on a regular basis.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff who set up usernames and passwords for e-mail, network access, <earning Platform and online Services access are working 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.

Malden Oaks
Investing in success

Dukes Centre
Dukes Avenue
Kingston KT2 5QY

020 8547 6711
020 8547 6660

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.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use RAv3 with its 2-factor authentication for remote access into our systems.
- We use the DfE S2S site to securely transfer CTF student data files to DfE / other schools.
- We use the Pan-London Admissions system to transfer admissions data. Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use LGfL AutoUpdate for creation of online user accounts for access to broadband services.
- We use LGfL's USO FX to transfer documents to schools in London, such as references, reports of children.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area/offices.
- All servers are in lockable locations and managed by DBS-checked staff.
- We use LGfL's GridStore remote secure back-up / named alternative solution for disaster recovery on our network / admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- 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.

Date agreed by the Management Committee:

Agreed date for Next Review: