

	<b>Name of School</b>	<b>Manor Primary School</b>
	<b>Policy review Date</b>	<b>September 2015</b>
	<b>Date of next Review</b>	<b>September 2017</b>
	<b>Who reviewed this policy?</b>	<b>Kate McGee &amp; Petra Collins (HT &amp; AHT/ICT Leader)</b>

**Policy: Managing Equipment**

**Using the school network, equipment and data safely: general guidance**

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides pupils with an individual network log-in username.
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after a few mins and have to re-enter their username and password to re-enter the network.];
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO

switch the computers off at the end of the day / we automatically remotely switch off all computers at 6 o'clock;

- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email; finance system; etc.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or SIMS Support through LA systems; Education Welfare Officers accessing attendance data on specific children.
- Provides pupils and staff with access to content and resources through the approved Learning Platform (MLE) which staff and pupils access using their Shibboleth compliant username and password.
- Uses our broadband network for our CCTV system and this has been set-up by approved LGfL partners;
- Uses the DfES secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.