Bushey Heath Primary School
Data Protection Policy

- At this school we have an Acceptable Use policy which is reviewed at least annually, which all staff sign. Copies are kept on file. We use the LA model policy.
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors. We use the LA model agreements.
- Safe Handling of Data Guidance documents are issued to all members of the school who have access to sensitive or personal data.

Protect and Restricted material must be encrypted if the material is to be removed from the school.

- At this school we encrypt flash drives for this purpose and limit such data removal.
- At this school we use <the DCSF S2S site> to securely transfer CTF pupil data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer, using <Outlook> <secure export to Local Authority Pupil Database>.

Protect and Restricted 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 CRB-checked staff.
- At this school we use follow LA back-up procedures and <lock the tapes in a secure cabinet>. <Back-ups are encrypted>. <No back-up tapes leave the site on mobile devices.>
- At this school we use <protocol> for disaster recovery on our admin server.

Disposal: Protect and Restricted 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 Authority's recommended current disposal firm <other named firm> for disposal of system hard drives where any protected or restricted data has been held.
- At this school paper based sensitive information is <shredded, using cross cut shredders>.
- <At this school we are using secure file deletion software>.
- 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 procedure>. <From 2009 all laptops have been set-up with laptop hard drive encryption>.

- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, SLG and Learning Platform access are controlled by <the LA processes, supported by the LA ICT Support Service> and / or by <name /role>.

- Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation.

27 April 2017