Information Security Guidelines for Staff at the Piggott School

All pupil data and staff data is personal information and as such falls under the Data Protection Act 1998, regardless of whether it is held electronically or on paper. The following guidelines on information security have been compiled after consultation within the Wokingham Borough Council. The Piggott School will ensure that all staff who hold or access personal information adhere to these guidelines. The School will continuously monitor and update our data protection policy and relevant procedures to reflect these guidelines.

All School staff are required to take the following measures into consideration when handling personal data, at school or in other locations:

- Particular care should be taken where personal data is kept, on paper or on a PC or laptop, in a place where pupils or staff may be present, e.g. a classroom. When leaving their computer, even for a few minutes, staff should lock the desktop (in Windows XP this can be done by pressing the Windows key and L). In case staff are called away urgently, a screen saver should be set to cut in after quite a short time (3-5 minutes) so that the data on the screen is made inaccessible to passers-by. The screen saver must be set so that staff have to type in a password to view the data again. Setting too short a cut-in time can become a nuisance, but staff should avoid the temptation to set an interval of more than, say, 10-15 minutes.

- Staff should avoid taking personal information home with them if at all possible, whether on paper, on a laptop or on removable storage media. A list of associated risks is given below.

- Holding any personal information on a laptop poses a security risk. The only way to eliminate this risk is if the laptop is fully encrypted. Any personal information which is placed on a laptop should be removed or deleted as soon as possible.

- Consider applying a BIOS password to PCs and laptops. This prevents any software (including the operating system, e.g. Windows XP) from loading without a password. The school's ICT technician/support should be able to help set this up.

- Logging into the network from elsewhere, eg home, could also pose a security risk. This should only be accomplished by using a secure, encrypted connection. An insecure connection will open up the school network to intruders.

- All removable storage media, e.g. memory sticks or CDs, pose a security risk. No personal information should be stored on such devices, unless they are encrypted. Staff individually have full responsibility for all removable devices in their possession, whether school or privately owned, e.g. memory stick, disc (CDs), mobile phone,

camera, camera card, portable hard drive, or any other unknown devices, and their contents whether downloaded by themselves or a third party, onsite or offsite.

- Should any content be offensive, considered unsuitable or be harmful to the system or School population, this will result in disciplinary action, and could lead to dismissal in the case of staff or exclusion in the case of students.

- If any of the above content is brought into School even unwittingly, by a pupil, parents or guardians and the Child Safeguarding Team will be informed. If it is brought in by a member of staff the necessary authorities will be notified. This can include the police, social services, the governing body and child protection agency.

- All removable devices should be checked for viruses prior to bringing on to site. Should staff or pupils not have current anti virus software on their computing equipment they should not bring any removable device into School.

- Should pupils or staff be identified as introducing viruses to the School system, the School reserve the right to remove access.

- Staff with access to the School system from home should not allow friends or family members to use their School allocated lap top unless IT has set up a special guest account.

- Staff must accept responsibility to consider the potential for harm to individuals if personal information is disclosed in an unauthorised manner, or if a laptop or removable media is stolen.

- Staff should take appropriate security measures to protect information from unauthorised loss, access or amendment and to reduce the risk of their laptop or removable media being lost or stolen.

- Staff should take reasonable precautions to ensure that the data is not accessed, disclosed or destroyed as a result of any act or omission on their part.

- Staff must never give out their passwords to anyone. As user names and passwords are often known or guessable by others, particular care needs to be taken with choice of passwords; a child's name or a pet's name should not be used. A number or a punctuation mark should also be used in the password e.g. Sn9wbi%d.

- Sensitive information provided to Governors should be marked confidential. Governors must take responsibility for the safe keeping of such documentation. Additionally Governors must ensure safe and secure disposal of all such documents.

I have read, understood and agree to abide by the above information security guidelines.

Signed..... Print name ..... Date .....