INFORMATION SECURITY GUIDELINES

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 Wokingham Borough Council. Please ensure that all staff who hold or access personal information adhere to these guidelines. Schools may wish to update their 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 (a few 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 the 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, e.g. 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 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. Do not use a child's name or a pet's name. Always include a number or a punctuation mark in the password, e.g. sn9wbi%d.

- Never send documents containing personal data by e-mail, e.g. to a home e-mail address or personal e-mail address. Web-based e-mail accounts such as hotmail and yahoo are particularly prone to unauthorised infiltration (hacking).
- Always have up to date virus scanning programs installed on laptops.
- Laptops should be kept constantly in view when travelling. The laptop should be placed on the floor, in the foot well or behind the driver's seat.
- Never leave laptops unattended in parked cars, not even in the boot.
- When travelling it is preferable to avoid using an obvious looking laptop case.
- Devices should be kept out of the public view as much as possible. If staff need to use it away from school then choose as private a place as possible.
- Inside non-public areas in school buildings, staff are encouraged to challenge people not known to them.

Using or accessing personal information at home, either electronically or on paper, makes it vulnerable to loss or unauthorised access. The most common risks are as follows.

- As a result of leaving papers in the house where they may be seen by other members of the family or by visitors.
- Theft of a laptop of briefcase from the home.
- Loss of a laptop or briefcase on the journey to/from work.
- Storage of information on removable media which is not encrypted.
- Theft or loss of removable media.
- Accidental access to information by a member of the family if it is stored on a household laptop or PC without protection.
- E-mailing information by means other than over a secure system.