WOOLLEY WOOD SCHOOL

DATA PROTECTION POLICY

Chair of Governors: C. A. Kirby

Headteacher: D Whitehead

Date: 15 September 2017

Date for review: September 2018

This document is available to Governors, Staff and can be accessed either by hard copy (located in School Office) or electronically in Staff Share on the school network

Each member of staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage. As a school we follow the "Seven Golden Rules of Data Sharing" (attached).

Data should:

■ Be kept in a locked filing cabinet, drawer, or safe;

or

■ If it is computerised, kept on a network drive that is regularly backed up and if a copy is kept on removable storage media e.g. memory stick or portable devices e.g. laptops, that media must itself be encrypted and kept in a locked filing cabinet, drawer, or safe.

If any data is to be taken from the school (e.g. to work at home) then the data must be held securely at all times whilst in transit and at the location it is being held. In particular, data must be protected from unauthorised access.

Ordinarily, personal data should never be stored at staff members' homes, whether in paper or electronic form, on laptop computers or other personal portable devices or at other remote sites.

All requests for information about children or staff at school must be discussed with the Senior Leadership Team. If a request is agreed details will be recorded in the office.

All requests made under the 'Freedom of Information Act' will be considered by a member of the Senior Leadership Team; advice from the Local Authority Legal Team will be sought if necessary, however the member of Senior Leadership Team will ensure that timescales are adhered to as set out in the legal framework of the Freedom of Information Act.

The following are acceptable types of documents to work on at home, due care should still be taken with the data storage and particularly transport (see above).

- Annual review education reports
- End of year reports
- IEPs
- Planning
- Observations

The only personal data recorded on these items is the names of the children

If any other types of documents may be taken home permission is required from the Senior Leadership Team. Extra care must be taken with these as they contain more personal information. Once they have been returned to school the only copies should be the ones stored and backed up on the **network drives**

If any form of data is lost, stolen or misappropriated (e.g. accounts being hacked) or if you suspect this has happened, the Headteacher must be informed immediately and an action plan will be devised.

Passwords for all school systems, including user logons and email accounts must not be shared with anybody. If they accidentally disclose their password the headteacher must be informed immediately and will perform a risk assessment and decide on action. It is a very serious matter if a staff member knowingly discloses or fails to report accidental disclosure of passwords and this will be investigated by the Senior Leadership Team.

Seven golden rules for information sharing

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. Consider safety and well-being:
Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure:
Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.