DATA PROTECTION 32

What does the law say?

The Data Protection Act 1988 requires that

- Anyone who records and uses personal information (data controllers) must be open about how the information is used and must follow the 8 principles of 'good information handling'.
- All individuals (data subjects) have certain rights, including the right to see information that is held about us and to have it corrected if it is wrong.

The rules of good information handling are:

All data controllers must follow the 8 data protection principles

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in line with the data subjects rights
- Secure
- Not transferred to countries outside of the EU without adequate protection

What is our policy on recording and access?

When recording information about pupils, staff should remember that:

- Parents have the right to see their children's records
- Students have the right to see their own records if they submit a request in writing. [Only if it is obvious that they do not understand what they are asking for, can the request be refused]

Upon a formal request to view data, staff must ensure that:

- Schools should not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else - including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

Upon a request to view data, the student's year tutor, in consultation with the respective member of the leadership team will examine the records and remove anything which can be construed as likely to cause serious harm to physical or mental health or which identifies other students.

What data do we need to keep secure?

1. All <u>personal data</u> which is not in the public domain, which personally identifies individuals **AND** the loss of which could cause harm or distress to that individual.

Personal data for adults		**Sensitive data**
Name, address, postcode, email, telephone numbers, driver licence numbers, date of birth	**combined with**	Bank details, mothers' maiden name, NI number, tax, benefits or pension details, health records, employment records, school attendance or records, anything

		related to criminal justice or child protection

Personal data for children		**Sensitive data**
Name, date of birth, email, registration group, year group, class group	**combined with**	Domestic: address, parents' first names, telephone number General school records e.g. attendance Assessment information SEN information Disciplinary records

2. Large databases, containing the personal data of large numbers of individuals. In general the larger the number of records, the higher the level of protection required.

How do we keep data secure?

1. Passwords for computer systems must not be recorded alongside user IDs or left on public display
2. Workstations and laptops should be left locked, and you should log out of the school's MIS before leaving a workstation or laptop.
3. In general sensitive data (see above) should not be emailed – email is inherently insecure
4. Sensitive information must not be placed in the bin – it should be passed to resources for shredding or securely deleted (on school laptops and workstations this deletion will happen when laptops are handed back when members of staff leave)
5. Students should not be allowed into the staff room where sensitive data and information may be on display

If in doubt, guidance about whether, and to what extent, pupils should be allowed access to their records can be sought from the Office of the Data Protection Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF (telephone 01625 545700) or by visiting https://ico.org.uk/

What do we share?

- Student data with Adviza – without permission
- Student data with the LA, DfE and other government agencies – without permission
- Confidential information with the MASH (safeguarding, Prevent) – informing parents except where to do so might endanger the young person

For more information, contact W Browne.

This policy is due for review by the end of May 2018.