DATA PROTECTION and the GDPR DRAFT April 2018

The following guidelines ensure that, as a school, we meet with the requirements of the General Data Protection Regulation (GDPR) that comes into force on May 25th 2018.

Terms

Data Controller - this is the school and its employees.

Data Processor - this is any party who processes data on the school's behalf.

✔ DO:

- Read and familiarise yourself with the Acceptable Use of ICT policy. Staff shared/policies/public
- Keep all data secure and only remove it from site **if necessary to fulfil your role**.
- Use your own user area, staff shared area to access documents using remote desktop from home.
- Record facts and professional opinions only on school records, emails and documents.
- Use strong passwords, i.e. a combination of 8 or more alphanumeric characters and symbols.
- Keep passwords to school systems safe and secure.
- No data should be held on data sticks or portable devices **unless they are encrypted.**
- **LOCK ALL WORK STATIONS OR LOG OFF when you leave them unattended for ANY period of time. (Windows L)**
- Be mindful of accessing systems if the computer is connected to a projector.
- Lock unoccupied offices and store rooms.
- Bring back all information taken for off-site trips and pass to SLA.
- Dispose of all personal/sensitive data in red bins.
- **Maintain a clean and tidy workspace, desk and classroom.**

✖ DO NOT:

- Share passwords.
- Store data on insecure removable drives
- Store data on the hard drive of any machine out of school
- Take student photographs on personal devices, use a school camera and refer to individual photograph permissions when necessary (stored on SIMs).
- Leave data and documents lying around in your classroom/staff room/car overnight….
- Discuss or share personal information with non-school staff unless they are linked professionals.

Taking / Using Data Off-Site

- Only take offsite information you are authorised to take and only take it when it is necessary.
- Ensure the information is protected, or limited from the view of others and is never left unattended.
- Do not dispose of sensitive hard copy at home; bring back to school and use red bins.
- Do not leave data/information/material in the car.
- Do not process data in a public space; train/café etc. **It is your responsibility to ensure you do not allow access to unauthorised users.**

SIMS, SISRA and all contain sensitive information, i.e. SEND needs, children in care and Pupil Premium students. When accessing these systems outside of school please be aware the data is only as secure as the end user allows. Do not leave any system logged on when you are not in front of the computer.

Email

We will be using encryption for some emails.

In the meantime you need to:

- Follow the Acceptable Use of ICT policy
- Use initials in subject lines – where the information is sensitive, use Confidential also in the subject line.
- Only send data spreadsheets by email when there is no alternative
- Use password protection on highly sensitive information that is regularly sent
- Send password in separate email
- Use common sense when sending information by email- avoid very highly sensitive information and minimise the risk by using forenames and initials in the body of the text.
- Maintain professional standards in all emails- these can be released as part of a Subject Access Request.

Printing

- Please be very aware of where printers are located when sending documents. Collect your printing straight away.
- Do not print sensitive data to a classroom printer – use an office printer or staffroom to minimise risk.
- If you believe you have found misplaced documents around the school building, please bring them to the main office.

Remember school may incur substantial fines for the loss or misuse of data (for each person affected- so the bigger the loss, the bigger the fine, the more sensitive the information, the bigger the fine) In theory up to £20 million or 4% of turnover.

Privacy Impact Assessments

- For any processing of data we should now conduct a privacy impact assessment- eg: Science want to buy a new piece of software for revision. The school would need to: Check that the processor is GDPR compliant/ensure the processor only has access to what is absolutely necessary/ make sure any consents were obtained and stored etc..
- Equally if the school refers a student to any external body, we would need verification that that 3rd party was GDPR compliant – ie we work with a number of charities- how do they store and dispose of data/who has access etc.

Inaccuracy:

- If you suspect data of being inaccurate, report it to Rob Carwood or Ben Vickers.

- Under the GDPR, individuals have a 'right to rectification.' All inaccuracies should be verified, rectified and it is also the school's duty to advise any third party which may have received incorrect data prior to rectification.

Breaches:

- Personal data breaches are those where misuse or loss data is likely to result in a risk to an individual's rights and freedoms, for example, risk of discrimination, damage to reputation, financial loss or loss of confidentiality.
- If you suspect or become aware of a data protection breach, this should be reported on the form available from B Vickers.

It may be necessary to report the breach to the Information Commissioners Office (ICO) if the loss or sharing of data has had a detrimental effect on an individual.

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

Subject Access Requests:

- Staff, students and parents can ask for any personal information the school holds in relation to them. Requests should be made via a "Subject Access Request". B Vickers will hold the forms.
- The GDPR specifies a one month timescale for handling requests and information. If a parent or subject requests information, you must pass that request to B Vickers immediately.
- In most cases, there can be no charge to provide data but the school may charge for requests that seem unfounded or are considered excessive. The school may also refuse excessive requests but must provide a reason for doing so. The school can decline a request where a previous SAR has been granted in the last 6 months.

Retention:

- Data relating to staff, students and school governance and finance is retained in line with the school's Record Retention Policy and Schedule
- Data is required to be retained for varying timescales depending on its use and should be archived securely where necessary. The policy should be consulted if staff are unsure as to retention requirements.

Disposal:

- Data must be disposed of securely via red bins**.**
- Disposal of expired student files, electronic data, SEND,CP, financial or governance data must only be disposed of by designated staff.

Relevant policies: Data Protection Policy (needs updating when the new bill is passed)
Record Retention Policy and Schedule
Acceptable use of ICT (staff)

Please see staff shared/policies for all school policies.
Further detailed guidance is available from the Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection

Consent

Where consent has been sought to process data for a particular purpose, it cannot be used for another purpose without consent being sought again.

There is a right to withdraw consent at any time and this should be straightforward and easy to do.

No consent is needed if:

- The data is being used for the prevention or detection of harm to a person or persons, ie safeguarding
- There is a legal obligation to obtain it, ie contact details
- There is a statutory obligation to pass the information on (eg: DfE)
- There is a legitimate purpose for processing data and this is made clear in our privacy notices (ie we share with SMHW so we can set homework)