REPORT

DPO report to governors

DATE REPORT COMPLETED	MAY 2020

OVERVIEW

We think we are compliant. Policy on the website. DPO in place (PK). All staff and parents have received privacy statements. We are cutting down radically on filing hardcopies and storing information on the cloud using MIS scholarpack. Hardcopies are seen as a weak point. A new high powered shredder was purchased to destroy when no longer required. This audit will be presented to the Governing Body in May 2020

THE CURRENT SITUATION

Steps taken so far to be GDPR-compliant

Actions:

- Privacy notices updated in May 2018 has been reviewed and remain unaltered.
- Procedures. Admissions information stored digitally. Password protected. All absence correspondence goes via the school secretary (DP) and is entered onto the MIS system. Hardcopies of both destroyed by the Data Processor (ES).
- Training to all staff was given on 4th September 2018. Universal safe guarding also touched on the importance of protection and what information can be shared. Email security of a sensitive mature destroyed. Principal and secretary use Anycomms to transfer sensitive information to schools and the LEA. Password protected files are also used with pay roll information.
- Risk Assessments now include a box to that must be ticked to indicate information taken out of school on trips and activities has returned to school. All trip consent forms are also shredded.
- All documents circulated to staff of a sensitive nature have GDPR sensitive at the top. Staff are asked to shred after use.

Our school's strengths

DPO and secretary have a good awareness of not storing unwanted data. All data sent is encrypted ANYCOMMS +

Our school's weaknesses

Continue that unwanted data is

Information regarding contacts and medical conditions of pupils on trips and swimming. Tightened up by including a return box on the Risk Assessment. Trip file in place that is returned to the office.

Updates from the sector

THE CURRENT SITUATION

As the GDPR is relatively new legislation, your DPO might update you on any new information that's been released since the last GDPR update you received – particularly if it affects your school at all. This might include new guidance from the Information Commissioner's Office or news of any data breaches at other schools.

Guidance given during INSET and safeguarding updates. 3rd Sept INSET 2019 will also include a GDPR update. Problem of sharing information needs to be sorted within the county as may schools still use files and hardcopies rather than encrypted or password protected electronic transfers.

DATA BREACHES

Summary of the breach	Reported to the ICO?	Type of data compromised	Action taken to make sure it doesn't happen again
Do not think we have breached the legislation	N/A	Personal details such as names and addresses have not been compromised by staff.	Training will be provided annually to remind about GDPR. Update of changes to our systems.

WHAT NEXT?

Upcoming challenges

Problem with a private school withholding information. Have put in a complaint to OFSTED and contacted MASH for guidance. Continue to ensure paper information entered digitally (MIS) is destroyed. Some schools still retain hard copies which are sent. This is insecure and a weakness of the system. LEA have been notified as yet no action.

Steps to be taken this term

Destruction of past information to apply with GDPR that has been stored within school. Reduce all hard copies.

In INSET cover the dangers of weak passwords and the use of USB pens and laptops. The norm is Staff work on sensitive information in school. Information is protected on the MIS.

We worked with our DPO expert Sharon Graham to produce this template. Sharon is DPO for 3 schools, and runs a GDPR working party for DPOs. She also has 10 years' experience in the education sector covering all aspects of operational management.