

DPO report to governors

DATE REPORT COMPLETED

MAY 2022

OVERVIEW

We think we are compliant. Policy on the website. DPO in place (PK). All staff and parents have received privacy statements. We are continuing cutting down on hardcopies and storing information on the cloud using MIS Scholarpack which is double password protected. We see hardcopies as a weak point. A new high-powered shredder was purchased to destroy paperwork which is no longer required. This audit will be presented to the Governing Body in May 2022

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 and is entered onto the MIS system. Hardcopies of both are destroyed by the Data Processor (JP).
- Training to all staff was given on 1st September 2021. Universal safeguarding 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 and are electronic. Staff are asked to shred after use if printed.

Our school's strengths

DPO and secretary have a good awareness of not storing unwanted data. All data sent is encrypted ANYCOMMS + or placed on Scholarpack which has limited access and is double password protected.

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

Guidance given during INSET and safeguarding updates. 1st Sept INSET 2021 (KCSE) will also include a GDPR update. Problem of some schools sharing information. This needs to be sorted within the county as many schools still use blue 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	NONE	Personal details such as names and addresses have not been compromised by staff.	Training will continue to be provided annually to remind about GDPR.

WHAT NEXT?

Upcoming challenges

Problem with a private school withholding information. Have put in a complaint to OFSTED in 2019 and contacted MASH for guidance. Continue to ensure paper information entered digitally (MIS) is destroyed. DFE Get Information About Pupils has been a useful addition to their website.

Steps to be taken this term

Destruction of past information to apply with GDPR that has been stored within school. Continue to 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.