FOREST PARK SCHOOL

Safeguarding Bulletin – 23rd September 2024

Safeguarding is Everyone's Responsibility

GDPR

GDPR - GDPR stands for 'General Data Protection Regulation.'

This comes from the Data Protection Act 2018 and relates to being responsible for the protection of data.

It is the responsibility of everyone to ensure data in school is protected and only information that is shared with outside agencies, is shared.

Every piece of personal data school hold must be:

- Processed lawfully, fairly and transparently
- Collected for specific, explicit and legitimate purposes
- Limited to what is necessary to achieve your purpose with it
- Accurate and kept up to date
- Held securely
- Only retained for as long as is necessary to achieve your purpose with it

School holds different data and information for all students and staff (personal, and sensitive/special data):

Personal Data	**Sensitive and Special Data**
Name	Usernames and passwords
Photos	Care plans
Parent's Evening Appointments	SEND documents
Report Letters	Union Trade membership
Meeting Requests	Biometrics (biological data)
Basic Medical Details	Individual health care records
Attendance letters	Religion
	Criminal record and disclosures
	Exclusions

Breach of data:

A data breach is where personal data is misused, misplaced or accessed inappropriately.
Data breaches in schools:

- Accidental loss or theft of equipment on which data is stored
- Human error – emails/post have been sent out by mistake
- Loss of data or equipment
- Malicious attacks – phishing
- Obtaining information by deceiving a member of staff
- Verbal - *please think about what you are discussing, is this necessary, should it be shared?*

Sensitive conversations should take place in private, not along corridors/in staffrooms or areas where others could overhear what is said.

Expectations of staff:
It is the responsibility of all staff to ensure data stored in school is protected.

To do this, you should:

- Respect the clean desk policy
- Lock work area when leaving
- Do not retain information that is NOT needed (shred immediately)
- Only use the information stored for its intended purpose (paper or on electronic systems)
- Obtain consent
- Password protect documents that are not in a secure folder
- Close down documents when they are not in use
- Only share documentation via secure emails
- Ensure all sensitive conversations are held in private, not in public areas
- Only transfer data on encrypted devices and check with IT
- Check that projectors in work areas are turned off when working on personal data
- Ensure any sensitive information (such as a student being PP, SEND etc) is hidden if the document can be seen by others in the room

Any breach of data, or concern that may have happened must be reported to the Headteacher in the first instance, and then the DPO – Data Protection Officer

Collating and saving information.

Student information is stored on many school systems inclusive of SIMS, Classcharts and CPOMS. Information regarding a student must only be shared with the named contacts on the student's SIMS account unless the member of staff is liaising with outside agencies such as police, social services etc. **Staff must always speak to the DSL/GDPR Lead and/or Pastoral Team before sharing any information about the students to outside agencies.**

At times, school may receive a request for documents to be shared such as a CPOMS report. **Requests of this nature must be passed onto the DSL who will liaise with the school's legal team.**

CPOMS

- Recordings should be made under the relevant category
- Recordings should be factual with no opinions (all information to be precise)
- Recordings in bullet point format
- All students involved in an incident or concern must be linked to the recording

The sharing of information regarding a child being at risk of significant harm can be shared without consent, only in "the best interests of the child" amongst relevant services.

Staff should speak to the DSL/GDPR Lead before **any** information is shared.

School Safeguarding Team Information:

Dawn Hindmarch – Designated Safeguarding Lead

Jackie Reynolds – Designated Safeguarding Lead

Jill Gray – Deputy Designated Safeguarding Lead

Tristan Coad – DPO – IT Systems

Whistleblowing Policy

If you have concerns regarding a member of staff, please refer to the Trust Whistleblowing Policy. Any concerns should remain confidential and reported to the Head Teacher. If the concern is about the Headteacher then this should be directed to the CEO.

All staff are requested to complete the additional training through The National College, using the following link:
https://nationalcollege.com/webinars/online-sexual-abuse-strengthening-safeguarding-measures