GDPR
Turton School is very active in our GDPR compliance. We are committed to ensuring we do the right thing for our Governors, our families, our students, our staff and the third parties we work with. Verified by a national law firm, we are focussed on ensuring our processes can be evidenced to demonstrate compliance.

Governance Structure and Data Protection Officer
Data privacy is discussed regularly at Governing Body meetings and reviewed by senior leaders within school.

Turton School's named Data Protection Officer is Cathy Bach (Deputy Head)

Data Mapping and Data Asset Register
We have completed a data mapping exercise. We know what data we have, why we have it, where it is held, how we access it and where we transfer it to.

Embedding Data Privacy into day to day life of the school – Training and Awareness
We have reviewed our Data Protection Policy to ensure that it complies with GDPR.

We have carried out training with our staff and Governors to ensure that:

- We know what we can do with data, and if unsure, we'll ask
- We are clear about how we're going to use data
- We protect the data we hold/process
- We ensure compliance, both individually and as a team

We have produced Privacy Notices for staff, students and parents, community users and School Direct trainees which explain what data we hold and what we do with it.

Information Security Risk
We have robust systems in place to manage our school network. This includes technical security measures (e.g. intrusion, detection, firewalls, monitoring), encryption of personal data, restricted access to personal data, protection of our physical premises and hard assets, maintaining security measures for our staff and regular testing of our security systems.

Third Party Risk and our Data Partners
Due diligence prior to working with a third party is key to ensure data has been gathered lawfully, and to ensure any data we share will be secure. If any third party partners need to comply with GDPR, we'll ensure they do.

Responding to individual complaints and data subject access requests (DSARs)
We already has a very robust process for dealing with consumer queries and subject access requests. This is a requirement under the Data Protection Act, therefore we are confident in our processes, which are tried/tested and we continually review for improvement. The key difference under GDPR is the timescale for response to a DSAR is reduced from 40 days to 30 days, which we do not foresee as an issue.

Data Privacy Breach Management Program
We have an effective data privacy incident and breach management plan, which we will continue to review and enhance as required.