GDPR Summary

The GDPR applies to all personal data that is held or processed. This can be data that is held electronically or on paper.

Personal Data

Personal data is defined as any information relating to an identified, or identifiable, individual. The legal definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data and online identifiers (eg usernames) and reflects the changes in technology and the way organisations collect and process information about people.

Even personal data that has been anonymised (or pseudonymised) can fall within the scope of GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Lawful Basis

There must be a lawful basis to process personal data. Most of data processing activities in school are conducted under either the basis of "public task" or "legitimate interest." All data processing activities need to be conducted properly in accordance with the appropriate guidelines maintaining the required protection and privacy for the individual(s) concerned.

Special Categories of personal data

The GDPR recognises that some personal data is particularly sensitive and so needs more protection. This is referred to as "special categories of personal data" and includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes, health – physical or mental, sex life or sexual orientation.

Personal data relating to criminal convictions and offences are not included as "special categories" but similar extra safeguards apply to its processing.

The GDPR has no special categories that are specific to the feelings, sensitivities and experiences of young people in school but the legislation does require that we are mindful of the potential or actual impact of any data breaches and the adverse effects these may have on the individual(s) concerned. With this in mind we should also consider very carefully the safeguards to maintain the security and privacy of the personal data we hold that could potentially cause upset or embarrassment to members of the student body.

Any data that relates to a child protection or safeguarding issue must be regarded as "special category" and afforded the highest level of data protection. As with all safeguarding issues the first port of call should be the DSL, Dawn Spence, or a member of her team.

Reporting data concerns and data breaches

It is critical that any risk to data security or data privacy is reported as soon as possible, and any data breach is reported immediately.

All issues around data protection, including data breaches, need to be communicated to the school's Data Protection Officer (DPO).

Currently the school's DPO is Tristan Ashman. tas@hws.haringey.sch.uk