iMap Education

School Policy

Section	School Policies
Policy Number	SP-020
Policy Name	Data Protection and GDPR Policy

Creation Date	Review date	Next Review date	Nominated Reviewer
15.07.16	01.09.21	August 2022	S Beddow

DATA PROTECTION AND GDPR POLICY

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils and parents.

1. Introduction:

This policy is written following guidance as set out by the DfE and Data protection: toolkit for schools, September 2018. iMap School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government comply with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this iMap so far as it reasonably practicable comply with the data protection principles, as contained in the data protection act.

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for specified and lawful purpose and shall not be processed in any manner not in line with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not to be kept for longer than is necessary for that purpose
- Be processed in accordance with the data subjects' rights
- Be securely protected from unauthorised access, accidental loss or destructions
- Be stored only in countries within the EU or with companies that comply with the EU's Data Protection Directive.

iMap School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy.

2. GDPR

The GDPR (General Data Protection Regulation) has replaced the Data Protection Act (DPA) and is set to strengthen and unify all data held within an organisation. For schools, GDPR brings a responsibility to inform parents and stakeholders about how they are using pupils' data and who it is being used by.

A great deal of the processing of personal data undertaken by schools will fall under a specific legal basis, 'in the public interest'. As it is in the public interest to operate schools successfully, it will mean that specific consent will not be needed in the majority of cases in schools.

GDPR will ensure data is protected and will give individuals more control over their data, however this means schools will have greater accountability for the data:

- Under GDPR, consent must be explicitly given to anything that isn't within the normal business of the school, especially if it involves a third party managing the data. Parents (or the pupil themselves depending on their age) must express consent for their child's data to be used outside of the normal business of the school.
- Schools must appoint a Data Protection Officer and be able to prove that they are GDPR compliant.
- Schools must ensure that their third party suppliers who may process any of their data is GDPR compliant and must have legally binding contracts with any company that processes any personal data. These contracts must cover what data is being processed, who it is being processed by, who has access to it and how it is protected.
- It will be compulsory that all data breaches which are likely to have a detrimental effect on the data subject are reported to the ICO within 72 hours.

3. Status of this policy:

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

4. The Data Controller and the Designated Data Controllers

The School as a corporate body is the Data Controller under the 1998 Act, and the Proprietor is therefore ultimately responsible for implementation. However, the Designated Data controllers will deal with day to day matters. The School has 2 Designated Data Controllers: They are the Principal and The Class Teacher.

Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be: The Principal.

5. Responsibilities for staff:

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the School of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a pupil's assessment data, opinions about their ability, references to other academic institutions, or details of personal circumstances), they must comply with the data protection act 1998.

6. Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely
- Personal information is not disclosed either orally, in writing, via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive an on a network drive that is regularly backed up; and
- If a copy is kept on a diskette or other removable storage media, that media itself be kept in a locked filing cabinet, drawer or safe.

7. Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the school holds and proce3swses about them or their child and why.
- Know how to gain access to it
- Know how to keep it up to date
- Know what the School is doing to comply with its obligations under the 1998 Act.

This policy document address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the *Subject Access Request* form and submit it to the Designated Data Controller.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provide within 40 days, as required by the 1998 Act.

8. Subject Consent

In many cases, the school can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the school processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.

Jobs will being the applicants into contact with children. The School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The school has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users. The school may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical conditions such as asthma or diabetes. The school will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

9. Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions or race. This may be to ensure that the School is a safe place for everyone. Because this is information considered **sensitive** under the 1998 Act, staff (and pupils where appropriate) will be asked to five their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

10. Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public Website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the school.

Examples of data

Personal Data

Definitions of personal data are highly complex, and it is difficult to define categorically. However, broadly speaking and in day-to-day use, 'persona data' is information which relates to a living, identifiable individual.

In the context of this document and the School's requirements to process 'personal data' as part of its duty of care and to educate pupils, 'personal data' may include:

- School admission and attendance registers;
- Pupil's curricular records;
- Reports to parents on the achievements of their children;
- Records in connection with pupils entered for prescribed public examinations;
- Staff records, including payroll records;
- Pupil disciplinary records;
- Personal information for teaching purposes;
- Records of contractors and suppliers.

If it is necessary for the school to process certain personal data to fulfil its obligations to pupils and their parents or guardians then consent is not required. However, any information which falls under the definition of personal data, and is not otherwise exempt

(see below) will remain, confidential. Data will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

Sensitive data may include:

- Ethnic or racial origin
- Political opinions
- Religious beliefs
- Other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Offence or alleged offence
- Proceedings or court sentence

Where sensitive personal data is processed by the School, the explicit consent of the appropriate individual will be required in writing.

11. Exemptions

Certain data is exempted from the provisions of the Data Protection Act, example include:

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the school.

There are other exemptions under the act.

12. Retention Data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons. Different categories of data will be retained for different periods of time. The time span can be requested in writing from School.

13. Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Sharepoint\general workspace\Company Policies & Procedures\iMap Services\School Policies