Data Protection Policy for Schools

Abstract

This policy aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, handled, stored and processed in accordance with the Data Protection Act 2018 (DPA 2018) and other relevant data protection related legislation.

Information belongs to the school regardless of location, for example at home, the cloud, or remote working and applies to all personal data collected, handled, stored, transmitted or shared. It therefore includes information held electronically on paper, or other physical media, which is shared electronically, physically, orally or visually.

This policy follows the Must, Why and How method and is designed to be read by all staff on a regular basis including at induction.

Legal basis

This policy meets the requirements of but is not limited to the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) and also meets the requirements of the following

- The Protection of Freedoms Act 2012 when referring to the use of biometric data.
- In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 (As amended in 2016), which gives parents the right of access to their child's educational record.
- The Freedom of Information Act (2000)
- The funding agreement and articles of association for Academies including Frees Schools.

Governance

The Data Controller

Our school is accountable for the processing of personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

We are registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and responsibilities

This policy applies to **all staff** employed by the school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

How to use this policy

Each individual policy aspect is listed below as an action. If you wish to know why or how we need to take these actions please click on the link to the other sections of the policy. This is policy is designed to be easy to access.

What we must do

1. ***MUST***: All employees must comply with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of natural individuals Why How
2. ***MUST***: Where personal data is in use we must make sure that data subjects have access to a complete and current Privacy Notice Why How

3. ***MUST:*** We must formally assess the risk to privacy rights introduced by any changes to new or existing systems or process which involves the use of personal data Why How
4. ***MUST***: We must process only the minimum amount of personal data necessary to deliver services Why How
5. ***MUST***: All employees who record opinions or intentions about pupils must do so carefully and professionally Why How
6. ***MUST***: We must take reasonable steps to ensure the personal data we hold is accurate, up to date and relevant Why How
7. ***MUST***: We must rely on consent as a condition for processing personal data only if there is no relevant legal power or other lawful condition Why How
8. ***MUST***: Consent must be obtained if personal data is to be used for promoting or marketing goods and services Why How
9. ***MUST***: Consent will expire at the end of each 'Key Stage' and will require renewal Why How
10. ***MUST***: We will ensure that the personal data we process is reviewed and destroyed when it is no longer necessary Why How
11. ***MUST***: If we receive a request from a pupil, parent or colleague asking to access their personal data, we must handle it as a Subject Access Request under the Data Protection Act 2018 or a request for the Education Record under the Education (Pupil Information) (England) Regulations 2005 where relevant Why How
12. ***MUST***: If we receive a request from anyone asking to access the personal data of someone other than themselves, we must fully consider Data Protection law before disclosing it Why How
13. ***MUST***: If someone requests we change the way we are processing their personal data, we must consider their rights under Data Protection law Why How
14. ***MUST NOT***: You must not access personal data which you have no right to view Why How
15. ***MUST***: You must follow system user guidance or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so Why How
16. ***MUST***: You must share personal data with external bodies who request it only if there is a current agreement in place to do so or it is approved by the Data Protection Officer or SIRO Why How
17. ***MUST***: Where the content of telephone calls, emails, internet activity and video images of employees and the public is recorded, monitored and disclosed this must be done in compliance with the law and regulatory Codes of Practices Why How
18. ***MUST***: All employees must be trained to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely Why How
19. ***MUST***: All employees are aware of the use of CCTV on our site and their obligations towards processing footage Why How
20. ***MUST***: Maintain an up to date entry in the Public Register of Data Controllers Why How
21. ***MUST:*** Where personal data needs to be anonymised or pseudonymised we must follow the relevant procedure Why How

22. ***MUST NOT***: You must not **share** any personal data held by us with an individual or organisation based in any country outside of the United Kingdom without seeking advice from the SIRO or Data Protection Officer Why How
23. ***MUST***: We must identify **Special Categories** of personal data and make sure it is handled with appropriate security and only accessible to authorised persons Why How
24. ***MUST***: When **sending** Special Category data to an external person or organisation, it should be marked as "OFFICIAL-SENSITIVE" and where possible, sent by a secure method Why How
25. ***MUST***: Report a data breach, even if only suspected or potential, immediately to the schools designated data protection lead Why How
26. ***MUST***: Report the intention to use a new or emerging technology to the Designated Data Protection Lead Why How
27. ***MUST***: Obtain written consent for photographs and videos to be taken of children for communication, marketing and promotional materials. We will clearly explain how images will be used Why How

Why we must adhere with this policy

1. To comply with legislation
2. To comply with Data Protection legislation which requires us to make the data subject aware of how we will handle their personal data
3. To ensure that the rights of the Data Subject are protected in any proposed new activity or change to an existing one
4. The law states that we must only process the minimum amount of information needed to carry out our business purpose. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate.
5. To maintain professional standards and to assist in defending the validity of such comments if the data subject exercises their rights to ask us to amend or delete their personal data if they feel it to be inaccurate.
6. To comply with a principle of Data Protection law
7. To comply with Data Protection law. Where processing does not rely on a legal condition other than consent
8. When using personal data for marketing and promoting services it is unlikely that any lawful condition other than consent would apply.
9. Consent, unless prescribed can only be valid for a reasonable period of time.
10. To comply with a principle of Data Protection law.
11. To comply with the right to access personal data
12. To comply with a principle of Data Protection law.
13. To comply with the rights of the Data Subject under Data Protection legislation

14. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so
15. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so
16. To comply with the legal requirements to keep personal secure but also to ensure that where there are legal grounds to share information in a managed way that this is done correctly.
17. The law permits organisations to hold such data in order to measure the quality of services being provided, to record consent etc. In certain circumstances recordings may be accessed, for example to investigate alleged criminal activity or breaches of organisational policy.
18. To comply with a principle in Data Protection law and the Data Protection Officer governance requirements
19. We adhere with Data Protection regulations when processing footage and the ICO Code of Practice for CCTV
20. This is a regulatory requirement and allows the public to see what personal information we hold to support transparency
21. Where personal data is used for research purposes, the processing of the data can be legitimised by provisions within Data Protection law
22. To comply with the right of the Data Subject to have equivalent legal safeguards in place over their data in another country as they would here.
Personal data transferred overseas (including hosted solutions) must be securely handled under the same or substantially similar provisions that exist under the Data Protection Act.
23. To comply with Article 9 of GDPR
24. To comply with Article 9 of GDPR and comply with a principle of Data Protection law requiring personal data is processed with appropriate security measures
25. ***MUST***: Report a data breach, even if only suspected or potential, immediately to the schools designated data protection lead
26. To comply with ICO guidance, to ensure a DPIA is carried out and to highlight potential risks to the school
27. To comply with Article 4 (11) of GDPR to ensure that the school holds a freely given, specific, informed and unambiguous indication of the data subjects wishes with a clear affirmation of intent.

How must we do this

1. By following all of the points in this policy
2. By approving, maintaining and making Privacy Notices available to the data subjects
3. By completing and approving a Privacy Impact Assessment, or Data Protection Impact Assessment where the processing is ‘high risk’ to the rights of the data subjects.

4. By ensuring that the means we use to gather personal data (such as forms etc) only ask for the information that is required in order to deliver the service
5. By considering that anything committed to record about an individual may be accessible by that individual in the future or challenged over its accuracy
6. For example, there should be at least an annual check of the currency of data held about service users and whenever contact is re-established with a service user, you should check that the information you hold about them is still correct
7. By ensuing that we hold relevant consents
8. By ensuring we hold relevant consents and checking marketing consents with a line manager
9. Parents/ Guardians of pupils in the last year of a key stage should expect a communication to ask them to refresh their consents. If they do not respond ahead of a deadline date then consent should be assumed to be no longer valid
10. We must review personal data regularly and delete information which is no longer required; although we must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the law allows us to keep indefinitely personal data processed only for historical, statistical or research purposes. The Retention Schedule will give guidance in these areas.
11. We must be aware that data subjects can ask others to make a request on their behalf. There must be evidence of consent provided by the Data Subject to support this.
12. Such requests would typically be managed under the Freedom of Information Act (if from a member of the public) or under Data Protection or Judicial law if for a criminal investigation, however the decision whether or not to disclose someone's personal data to a third party must satisfy the requirements of Data Protection law
13. By reviewing the impact of any requested change on any statutory duty being fulfilled by the Organisation.
14. By being aware through training and guidance from your manager on what information is appropriate for you to access to do your job. Systems and other data storage must be designed to protect access to personal data. You must inform your manager if you have access to data which you suspect you are not entitled to view.
15. By ensuring appropriate security controls are in place and rules to support those controls are followed. The following should be in place:

- technical methods, such as encryption, password protection of systems, restricting access to network folders
- physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure; and organisational measures, such as regular training and robust security
- Providing appropriate induction and training so that staff know what is expected of them
- Taking reasonable steps to ensure the reliability of staff that access personal data, for example, by the use of Disclosure and Barring Service (DBS) checks.
- Making sure that passwords are kept secure, forced to be changed after an agreed period and are never shared

16. Consult your manager, any procedure guidance or any library of sharing agreements managed by the Organisation. Consult the Data Protection Lead in one-off cases of sharing
17. By ensuring that employees and members of the public are fully aware of what personal data is being recorded about them and why, and it what circumstances that data may be used. Operation of overt surveillance equipment such as CCTV must always be done in line with relevant guidance. Any covert surveillance must be done in line with the provisions in the Investigatory Powers Act (2016)
18. By completing compulsory training courses relevant to your role. Records will be kept of induction training and annual refresher training. Training content for each role will be determined by feedback on current training methods and the outcome of investigating security incidents. This will be reviewed frequently.
19. CCTV governance measures are in places, access logs are maintained, impact assessments are held and regular reviews are conducted
19. By ensuring an Impact Assessment has been approved for the activity
20. The entry should be reviewed annually and an update is to be made when any change to the purposes of processing personal data occur
21. Follow Data Minimalisation guidance by only using the information that is strictly necessary
22. Consult the Data Protection Officer over any proposed sharing outside of the UK. If you are a manager who is proposing a change to or implementing a new system which may involve the hosting of personal data in a nation outside the UK, this must be first assessed by a DPIA which must be approved by your Headteacher
23. Special Categories of Personal Data are information revealing *racial or ethnic origin*, *political opinions*, *religious or philosophical beliefs*, or *trade union membership*, *genetic data*, *biometric data* for the purpose of uniquely identifying an individual, *data concerning health* or *data concerning an individual's sex life or sexual orientation*. Where this data is held it should be stored securely and in a way that access is restricted only to those internal staff that have a valid need to access it. It should only be shared externally after verifying that the recipient is entitled to access this data and through secure means
24. Hard-copy packages must be marked as such by writing on the exterior of the package. Emails should contain the wording in the 'subject' field before the email title. Refer to the Records of Processing Activity document and the register of Data Flows for clear instruction on how you are expected to handle sending the data securely according to the particular activity you are undertaking
25. Immediately to the schools designated data protection lead, Headteacher or most senior available officer with any relevant information held either electronically or physically
26. Carry out a DPIA with the schools Designated Data Protection Lead
27. Collect consent regularly via the school's admissions process and with bespoke forms for specific purposes

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in
place, please raise a formal request by contacting the Headteacher

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Glossary

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including 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
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data. (School)
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. (Includes contractors, the Council, & Examination body)
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.