Scholes (Elmet) Primary
St James' CE Primary
Moortown Primary

Data Protection Policy

This Policy is reviewed annually (or sooner if required) by the Data Protection Officer and the Policies Committee and approved by the Governing Board.

This Policy was last updated February 2021.

For ease of reference and understanding, the first part of this Policy is a summary of the main points and practices with links to further external information and appendices to this Policy.

Contents

INTRODUCTION

This Data Protection Policy has been created under current data protection legislation and guidance as per the statement from the UK Information Commissioner on 29 January 2020.

When the UK left the European Union on 31 January 2020 it entered a "Brexit Transition period" which ends on 31 December 2020. During this period it is "business as usual" for data protection.

Once the Transition period has ended there will be some changes to the UK data protection legislation and guidance will be issued by the relevant regulatory bodies. Sphere Federation's Data Protection Officer will be monitoring these changes and where applicable this Policy will be updated accordingly.

1. POLICY STATEMENT

This Data Protection Policy is Sphere Federation's ("the Federation") statement of how personal data is protected through an agreed and adopted set of principles, rules and guidelines which ensure ongoing compliance with data protection legislation, codes and guidance.

1.1. The Federation is committed to ensuring all personal data collected about staff, pupils, parents, carers, governors, visitors and other individuals is collected, stored, maintained, processed and disclosed in accordance with the appropriate data protection legislation.

1.2. This Policy applies to all personal data regardless of whether it is in paper or electronic format.

2. ABOUT THIS POLICY

2.1. This Policy, and any other documents referred to in it, sets out the Federation schools' approach to compliance with the appropriate data protection legislation and codes by meeting the requirements of, amongst others, the UK Data Protection Act 2018 ("DPA 2018") the EU General Data Protection Regulation 2016/679 ("GDPR"), and the Age Appropriate Design Code ("Childrens Code").

2.2. This Policy does not form part of any employee's contract of employment and may be amended at any time. However, it is essential that all staff are aware of the data protection requirements and so is included in the staff handbook.

2.3. This Policy has been approved by the Data Protection Officer ("DPO"), the Federation's Policy Committee and Governing Board.

3. LEGAL FRAMEWORK

This Policy meets and complies with the requirements of the following:

3.1. The GDPR and DPA 2018 based on the Guide to the GDPR published by the Information Commissioner's Office (ICO), the UK's Supervisory Authority, also referred to as the Data Protection Authority.

3.2. The Protection of Freedoms Act 2012 when referring to the Federation schools' use of biometric data and reflects the ICO's CCTV Code of Practice for the use of surveillance cameras and personal information.

3.3. Regulation 5 of the Education (Pupil Information) (England) Regulations 2005 (as amended in 2016) which gives parents or those with parental authority the right of access to their child's educational record.

3.4. Each individual school within the Federation is registered as a Data Controller with the ICO.

4. DEFINITION OF TERMS

Set out below are some of the terms used in this Policy together with a brief explanation as to what they mean. Further explanatory definitions and details are in Appendix 1 to this Policy which can be easily accessed by the relevant hyperlinks.

4.1. Personal Data means any information about a living individual ("Data Subject") examples of which could include the individual's name, address, identification number, pupil's attendance, special educational needs requirements or photographs.

4.2. Special categories of Personal Data ("Sensitive Data") is personal data which is more sensitive and so needs more protection.

4.3. Processing is anything done with or to personal data in a specific way such as collecting, recording, organising, structuring, storing or destroying the data. This can be automated or manual. Any processing must be carried out under a lawful basis.

4.4. Data Subjects is the technical term for identified or identifiable living individuals whose personal data is held or processed.

4.5. Data Controller is a person or organisation who determines how and why the personal data is held or processed. Each school within the Federation is a data controller in its own right because it processes personal data relating to parents, those with parental authority, pupils, staff, Governors, visitors and others.

4.6. Data Processor is a person or other body, who is not an employee of the Data Controller, who processes personal data on behalf of the Data Controller.

4.7. Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. ROLES AND RESPONSIBILITIES

This Policy applies to all staff employed by the Federation schools and to external organisations or individuals working on the schools' behalf. Staff who do not comply with this Policy may face disciplinary action.

5.1. Governing Board

The Governing Board has overall responsibility for ensuring that the Federation schools comply with all relevant data protection obligations.

5.2. Data Protection Officer ("DPO")

a The DPO is an independent, expert in data protection, adequately resourced and reports to the highest management level.

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

c The Federation schools' DPO is:

Mr Richard Lewis-Ogden
Tel: 0113 336 8400
Email: dataprotection@carrmanor.org.uk

5.3. Headteacher

The Headteacher acts as the representative of the data controller on a day to day basis.

5.4. All Staff

Staff are responsible for:

a Collecting, storing and processing any personal data in accordance with this policy;

b Informing their school of any changes to their personal data, such as a change of address;

c Contacting the DPO in the following circumstances:

i With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;

ii If they have any concerns that this Policy is not being followed;

iii If they are unsure whether or not they have a lawful basis to use personal data in a particular way;

iv If they need to rely on or obtain consent, require a Privacy Notice, receive a data protection rights request from an individual, or transfer personal data outside the EEA;

v If there has been a personal data breach;

vi Whenever they are engaging in a new activity that may affect the privacy rights of individuals;

vii If they need help with contracts or sharing personal data with third parties

6. DATA PROTECTION PRINCIPLES

Everyone responsible for using personal data must follow strict rules known as the "Data Protection Principles". There are 7 key principles, which are the same in both the DPA 2018 and the GDPR:

6.1. Lawfulness, Fairness and Transparency - personal data must be processed lawfully, fairly and in a transparent manner.

6.2. Purpose Limitation - personal data must be collected for specified, explicit and legitimate purposes.

6.3. Data Minimisation - personal data collected must be adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.

6.4. Accuracy - personal data must be accurate and where necessary, kept up to date.

6.5. Storage Limitation - personal data must be kept for no longer than is necessary for the purposes for which it is processed.

6.6. Integrity and Confidentiality (Security) - personal data must be processed in a way that it ensures it is appropriately secure.

6.7. Accountability - The school is responsible for what is done with personal data ensuring compliance with the principles and must have appropriate measures and records in place to be able to demonstrate compliance.

This Policy sets out how the school complies with these Principles.

7. DATA SUBJECT RIGHTS

7.1. There are 8 main individual rights in both the GDPR and DPA 2018, brief details of which are noted below. The timescales for responding to any requests under any of the rights are that they must be dealt with as soon as possible and within 1 calendar month starting from the date of receipt of the request.

a The right to be informed - to be informed about how your data is being used and processed

b The right of access - access to personal data using through a Subject Access Request ("SAR")

c The right to rectification - have inaccurate data corrected

d The right to erasure - have data deleted

e The right to restrict processing - to stop or restrict the processing of your data

f The right to data portability - allowing the individual to obtain and re-use their personal data for different services

g The right to object - object to how the individual's data is used in certain circumstances

h Rights in relation to automated decision making and profiling - automated decision making processes (without human involvement) and profiling, for example to predict behaviour or interests

7.2. Children have the same rights as adults over their personal data with additional child specific considerations. These can be found in the Children and GDPR Guidance provided by the ICO, which sits alongside their data protection guide, providing more detailed and practical guidance for those organisations who are processing childrens' personal data.

7.3. Individuals should submit any request to exercise any of these rights to the DPO. If any member of staff receives such a request they must immediately forward it to the DPO.

8. SUBJECT ACCESS REQUESTS ("SARs")

8.1. Individuals, or a third party on their behalf, have a right to make a SAR to gain access to their personal data, and any supplementary information that the school holds about them. Wherever possible, SARs should be submitted in writing, either by letter, email or fax to the Headteacher or the DPO and include:

a Name of the individual

b Correspondence address

c Contact number and email address

d Details of the information required

Before the information is provided the school will be asking for 2 forms of identification.

If staff receive a SAR they must immediately notify their line manager and the DPO.

8.2. Children and SARs

a Personal data about a child belongs to that child and not the parents or those with parental authority. For a parent or those with parental authority to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent.

b Children below the age of 12 are generally not thought of as being mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or those with parental authority of pupils at the school may be granted without the express permission of the child. This is not a rule and a pupil's ability to understand their rights will always be judged on a case by case basis.

9. RESPONDING TO SARs

The school has a procedure for responding to SARs which can be found in Appendix 3 of this Policy.

10. EDUCATIONAL RECORDS

10.1. Parents or those with parental authority/ have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

10.2. Wherever possible, any request should be submitted in writing, either by letter, email or fax to the Headteacher or the DPO. If any member of staff receive such a request, they must immediately forward it to the DPO.

11. BIOMETRIC RECOGNITION SYSTEMS

11.1. Pupils

a Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18

b If pupils' biometric data is used as part of an automated biometric recognition system (eg pupils use finger prints to receive school dinners instead of paying with cash) the school complies with the Protection of Freedoms Act 2012, the DPA 2018 and GDPR.

c Parents or those with parental authority will be notified before any biometric recognition system is put in place or before their child first takes part in it and the school will obtain written consent from them before any biometric data is taken from the child and first process it.

d Parents or those with parental authority have the right to choose not to use the school's biometric system(s) and in those cases alternative means of accessing the relevant services will be provided.

e If at any time a pupil refuses to participate in, or continue to participate in anything that involves the processing of their biometric data or otherwise objects to the processing of that information, that data will not be processed irrespective of any consent given by the pupil's parent or those with parental authority. (Protection of Freedoms Act 2012)

11.2. Staff

a Where staff members or other adults use the school's biometric recognition systems, their consent will be obtained before they first take part in it or alternative means of accessing the service will be provided if they object.

b Staff members and other adults can withdraw consent at any time and the school will delete any relevant data already captured.

12. CCTV

12.1. CCTV is used in various locations around the Federation schools' sites for safety purposes.

12.2. The school does not need to ask individuals' permission to use CCTV, but it is made clear where individuals are being recorded.

12.3. Security cameras are clearly visible and accompanied by prominent signs that CCTV is in use.

12.4. The school adheres to the ICO Code of Practice for Surveillance Cameras & Personal Information

12.5. All enquiries about the CCTV system should be directed to the Sphere Federation Resources Managers or DPO

13. PHOTOGRAPHS AND VIDEOS

As part of the school's activities, photographs may be taken and images recorded within the schools.

13.1. The legal basis for this is for the purpose of identifying pupils.

13.2. Written consent will be obtained from parents or those with parental authority for photographs and videos to be taken of their child for communication, marketing and promotional materials.

13.3. It will be clearly explained to the pupils and parents or those with parental authority how the photographs and / or videos will be used.

13.4. Where parental consent is not required it will be clearly explained to the pupil how the photographs and / or videos will be used.

13.5. Uses may include:

a Within school on notice boards and in school magazines, brochures, newsletters etc

b Outside of school by external agencies such as the school photographers, newspapers, and for marketing campaigns.

c Online on the school's website or social media pages.

d When using photographs and videos in this way they will not be accompanied by any other personal information about the child to ensure they cannot be identified

13.6. Consent can be refused or withdrawn at any time. If consent is withdrawn the photographs and / or videos will be deleted and not distributed any further.

13.7. Pupils and parents or those with parental authority will not be permitted to take photographs or make videos other than for their own personal and domestic use. Such photographs and videos will not be shared publicly - eg via social media

14. AGE APPROPRIATE DESIGN CODE ("CHILDREN'S CODE")

14.1. The Children's Code is a statutory code of practice under the DPA 2018 requiring organisations to provide better online privacy protections for children, up to the age of 18.

14.2. Issued on 12 August 2020, it came into force on 2 September 2020, triggering a 12 month transition period to enable the appropriate organisations to make the necessary changes to put childrens' privacy at the heart of their design.

14.3. From the ICO's statement on 2 September 2020 "The code breaks new ground as regulatory guidance focused on a 'by design approach' and is a huge step towards protecting children online, especially given the increased reliance on online services at home during COVID-19…. All the major social media and online services used by children in the UK will need to conform to the code"

15. SHARING PERSONAL DATA

The school will not normally disclose or share personal data but, where it is necessary, individuals will be informed in accordance with this Policy. There are however some bodies with whom personal data is routinely shared for the purposes of the schools being able to carry out their legitimate busines. These as listed in the attached Appendix 2 together with those additional ad hoc exceptions, together with the reasons.

16. DATA PROTECTION BY DESIGN AND DEFAULT

Measures are in place to show that the school has integrated data protection into all data processing activities, including:

16.1. The appointment of a suitable DPO

16.2. Only collecting and maintaining necessary data to enable the school to fulfil their tasks

16.3. Only processing data that is necessary for each specific purpose

16.4. Completing Data Privacy Impact Assessments (DPIAs) where required under the advice of the DPO

16.5. Integrating data protection into all policies and notices

16.6. Regularly training members of staff on data protection laws and guidance and keeping a record of attendance.

16.7. Regularly conducting reviews and audits to test the privacy measures to ensure compliance.

16.8. Maintaining records of processing activities

17. DATA SECURITY AND STORAGE OF RECORDS

The school has processes in place to protect personal data from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage.

18. DISPOSAL OF RECORDS

Personal data will be disposed of securely where:

18.1. It is no longer required

18.2. It has become inaccurate or out of date and cannot be or does not need to be rectified or updated.

19. PERSONAL DATA BREACHES

19.1. The school will take all reasonable endeavours to ensure there are no personal data breaches.

19.2. Should there be a suspected data breach, the procedure set out in Appendix 4 will be followed.

19.3. If necessary the data breach will be reported to the ICO within 72 hours of becoming aware of it by the DPO.

20. TRAINING

20.1. All members of staff and Governors are provided with data protection training as part of their induction process.

20.2. Data protection forms part of the continuing professional development, where changes to legislation, guidance or the school's processes makes it necessary.

21. MONITORING ARRANGEMENTS

21.1. The DPO is responsible for monitoring and reviewing this Policy.

21.2. This policy will be reviewed annually (or earlier if required) by the DPO and the Federation's Policies Committee in accordance with the DfE's Guidance on Statutory Policies before being put to the Governing Board for approval.

21.3. Next scheduled review date November 2021.

22. LINKS WITH OTHER POLICIES

This Data Protection Policy is linked to the Federation schools' policies including:

22.1. Freedom of Information Policy

22.2. Online Safety Policy and the accompanying Acceptable Use Policies

22.3. Safeguarding and Child Protection Policy

22.4. Data Processing Agreement (Adept)

22.5. Record Retention Policy

22.6. Privacy Notices

22.7. Staff Code of Conduct

22.8. Acceptable use of ICT / Digital technology Policy

As well as legislation and guidance as provided by external bodies such as the Department for Education, Leeds City Council and the Information Commissioner's Office.

APPENDIX 1

GLOSSARY

Age Appropriate Design Code ("Childrens Code")	The Children's Code applies to organisations providing online services and products likely to be accessed by children and the transition period gives organisations a year to make the necessary changes to put children's privacy at the heart of their design. Defined in the ICO Age Appropriate Design Code - a code of practice for online services: "This code applies to "information society services ("ISS") likely to be accessed by children" in the UK. This includes many apps, programs, connected toys and devices, search engines, social media platform, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet. It is not restricted to services specifically directed at children."
Data Protection Act 2018 ("DPA 2018")	The DPA 2018 is the UK's implementation of the GDPR and became enforceable on 25 May 2018, the same time as the GDPR. The UK left the EU on1 January 2020 entering into a transition period which ends on 31 December 2020 with the GDPR being retained in UK domestic law but with the UK having the independence to keep the framework under review. At the end of the transition period the GDPR will be brought into UK law as the "UK GDPR" with the DPA 2018 which currently sits alongside the GDPR and tailors the GDPR within the UK will continue to apply.
Data Controller	The role of the Data Controller is basically to be the manager of personal data, responsible for deciding who is allowed to do what with it and how it is done to ensure compliance with data protection laws. Data Controllers are registered with, and pay a data protection fee to the ICO. There is quite often confusion with regards to the definition of a Data Controller and Data Processor. The ICO have produced a guide to explain the difference which can be found here.
Data Controller Registrations	The registration for each school is renewed annually or otherwise as legally required: Data Controller: Moortown Primary School Registration No: Z1580847 Date Registered: 20 January 2009 Renewal Date: 19 January 2021 Data Controller: Scholes (Elmet) Primary School Registration No: Z8484991 Date Registered: 01 March 2004 Renewal Date: 28 February 2021 Data Controller: St James CE Primary School Registration No: Z7190857 Date Registered: 12 November 2002 Renewal Date: 11 November 2021
Data Processor	A Data Processor is defined by both the GDPR and DPA 2018 as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority."

	As noted above, there is quite often confusion with regards to the positions of Data Controllers and Data Processors. The ICO have produced a guide to explain the difference which can be found here.
Data Protection by Design and Default	The GDPR and DPA 2018 require measures to be in place to show data protection is integrated in all data processing activities, including: • The DPO is suitably qualified and has the necessary resources to fulfil their duties and maintain their expert knowledge; • Only processing personal data that is necessary for each specific purpose of processing and always in line with the Data Protection Principles set out in the relevant data protection law; • Completing DPIAs where the school's processing of personal data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process); • Integrating data protection into internal documents including this Policy and any related policies and notices; • Regularly training members of staff on data protection law, this Policy, any related policies and any other data protection matters, keeping a record of attendance; • Regularly conducting reviews and audits to test the school's privacy measures and ensure compliance; • Maintain records of processing activities, including: - For the benefit of individuals, making available the name and contact details of the schools, DPO and all information required to be shared about how the school uses and processes their personal data (via the Privacy Notices); - For all personal data held, maintaining an internal record of the type of data, data subject, how and why the data is being used, any third-party recipients, how and why the data is being stored, retention periods and how the data is being kept secure.
Data Protection Officer	The DPO is: • responsible for overseeing the implementation of this Policy, monitoring compliance with appropriate data protection law and developing related policies and guidelines where applicable • responsible for providing an annual report of their activities directly to the Governing Board and, where relevant, provide the Board with advice and recommendations on Federation data protection issues Full details of the DPO's responsibilities are set out in our service level agreement with the data protection support provider.
Data Protection Principles	Lawfulness, fairness and transparency The school will only process personal data where is has one of the "lawful bases" (legal reasons) to do so under data protection law: • Consent - The individual (or their parents or those with parental authority, when appropriate, in the case of a pupil) has freely given clear consent to process their personal data for a specific purpose • Contract - The processing is necessary so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract • Legal Obligation - The processing is necessary so that the school can comply with the law (not including contractual obligations) • Vital Interests - The processing is necessary to protect the individual eg someone's life

	• Public Task - The processing is necessary so that the school, as a public authority, can perform a task in the public interest to carry out its official functions which have a clear basis in law • Legitimate Interests - The processing is necessary for the legitimate interests of the school or third party, providing the rights and freedoms of the individual are not overridden. For special categories of personal data, as defined in the DPA 2018 and the GDPR, processing will only be carried out if explicit consent of the individual (or parents or those with parental authority, when appropriate, in the case of a pupil), unless reliance on consent is prohibited by EU or member state law. Whilst the majority of the digital systems used in school are to support the teaching and learning of the pupils, and therefore the school has a legal basis for processing, there may be times when other tools are used. Where such online services are offered to pupils, the school relies on consent as the basis for processing and parental consent is obtained (except for online counselling and preventative services). Wherever personal data is firstly collected directly from individuals, they are provided with the relevant information required by data protection law. Staff will only process personal data where it is necessary in order to do their jobs.
	Purpose limitation Personal data shall only be used for specific explicit and legitimate reasons. These reasons will be explained to the individuals when their data is first collected. If it is required to use the personal data for reasons other than those given when it was first obtained, the school will inform the individuals concerned before it is done and will seek consent where necessary.
	Data minimisation Personal data shall only be used in a way that is adequate, relevant and limited to only what is necessary
	Accuracy Personal data shall be accurate and, where necessary, kept up to date by taking appropriate steps such as data verification exercises
	Storage limitation Personal data is kept for no longer than is necessary. When staff no longer need the personal data they hold, they will ensure it is deleted or anonymised. This will be done in accordance with the school's Record Retention Policy.
	Integrity and Confidentiality (Security) Personal data is handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
	Accountability Responsibility for what is done with the personal data and compliance with the other principles. There must be appropriate measures and records in place to be able to demonstrate compliance.
Data Security and Storage	Personal data is protected and kept safe from unauthorised or unlawful access, alteration, processing or disclosure against accidental or unlawful loss, destruction or damage. In particular

	• Paper-based records and portable electronic devices such as laptops and hard drives that contain personal data are kept under lock and key when not in use. • Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables or anywhere else where there is general access. • Where personal information needs to be taken off site. • Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals and not reuse passwords from other sites. • Encryption software is used to protect all portable devices and removable media such as laptops and USB devices. • Staff, pupils or Governors who store personal information on their personal devices are expected to follow the same security procedures as for school owned equipment. • Where the school needs to share personal data with third parties, due diligence is carried out and reasonable steps taken to ensure it is stored securely and adequately protected.
Data Subjects	The identified or identifiable living individual to whom personal data relates.
Data Subject Rights	In addition to the main rights (detailed below) individuals also have the right to: • Withdraw their consent to processing at any time • Prevent the use of their personal data for direct marketing purposes • Challenge processing which has been justified on the basis of public interest • Be notified of a data breach in certain circumstances • Make a complaint to the ICO As well as the individual's main rights, any organisation handling data must: • ensure that the appropriate technical and business security measures are in place to safeguard personal data • ensure that personal data is not transferred abroad without suitable safeguards • treat individuals justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information • set out clear procedures for responding to requests for information and therefore the school will comply with these requirements.
	Right to be informed Individuals have the right to • be informed about the collection and use of their personal data; • be provided with information including the purposes for processing their personal data, retention periods for the personal data and who it will be shared with, collectively known as "privacy information" as defined by the ICO • be provided with the privacy information at the time of direct collection of their personal data • be provided with the privacy information within a reasonable time and within 1 calendar month of receipt of an individual's personal data from other sources

	• be provided with all information in a clear, concise, transparent and intelligible manner There are a few occasions where it is not necessary to provide privacy information, eg if the individual already has the information or it would involve a disproportionate effort to provide it to them. Children must be provided with the same information as adults. Further details of how these should be considered can be found here.
	Right of access • Individuals have the right of access and to receive a copy of their personal data and other supplementary information, including: - confirmation that their personal data is being processed - access to a copy of their personal data - the purposes of the data processing - the categories of personal data concerned - who the data has been or will be shared with - how long the data will be stored for, or if this is not possible, the criteria used to determine this period - the source of the data if not the individual - whether any automated decision-making is being applied to their data, and what the significance and consequences might be for the individual - where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing - the right to lodge a complained with the ICO or another supervisory authority - the safeguards provided if the data is being transferred internationally The school has a procedure for responding to SARs details of which can be found in Appendix 3 attached to this Policy.
	Right to rectification • Individuals have the right to have inaccurate personal data rectified or completed if incomplete; • The request for rectification can be made verbally or in writing; • The request must be responded to as soon as possible and within 1 calendar month from the date of receipt • In certain circumstances the right can be refused; • This right is closely linked to the data controller's obligations under the Accuracy Principle.
	Right to erasure • Individuals have the right to have their data erased, also known as the "right to be forgotten"; • The request can be made verbally or in writing; • This right is not absolute and only applies in certain circumstances; • The request must be responded to as soon as possible and within 1 calendar month from the date of receipt • This right is not the only way in which the data protection legislation places an obligation on the data controller to consider whether to delete personal data.
	Right to restrict processing • Individuals have the right to request the restriction or suppression of their personal data;

	• This is not an absolute right and only applies in certain circumstances; • When processing is restricted it is permitted to store the personal data but not use it; • The request can be made verbally or in writing; • The request must be responded to as soon as possible and within 1 calendar month from the date of receipt.
	Right to data portability • Individuals have the right to obtain and reuse their personal data for their own purposes across different services; • It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way without affecting its usability; • This right only applies to personal data an individual has provided to a data controller; • The request can be made verbally or in writing; • The request must be responded to as soon as possible and within 1 calendar month from the date of receipt.
	Right to object • Individuals have the right to object to the processing of their personal data in certain circumstances; • Individuals have an absolute right to stop their personal data being used for direct marketing purposes; • In other cases, where the right to object applies, the data controller may be able to continue processing if it can be shown they have a compelling reason for doing so; • Individuals must be informed about their right to object; • The request can be made verbally or in writing; • The request must be responded to as soon as possible and within 1 calendar month from the date of receipt.
	Rights relating to automated decision making including profiling • The GDPR has provisions on: - Automated individual decision making (making a decision solely by automated means without any human involvement); - Profiling (automated processing of personal data to evaluate certain things about an individual); - Profiling can be part of an automated-decision making process. • There are additional rules to protect individuals if the data controller is carrying out automated-decision that has legal or similarly significant effects on them which requires - Individuals are provided with information about the processing; - Provide simple ways for individuals to request human intervention or to be able to challenge a decision; - The data controller must carry out regular checks to ensure the systems are working as intended. • The request must be responded to as soon as possible and within 1 calendar month from the date of receipt.
Disposal of records	• Personal data that is no longer needed will be disposed of securely.

	• Personal data that has become inaccurate or out of date will also be disposed of securely where it cannot or does not need to be rectified or updated. • For example: - Paper based records will be shredded or incinerated; - Electronic files will be overwritten or deleted. • Third parties may be used to safely dispose of records on the school's behalf. If so, the third party will be required to provide sufficient guarantees that it complies with data protection law.
GDPR	The General Data Protection Regulation (EU) 2016/679 (GDPR) is a data protection and privacy law which was drafted and adopted by the EU in 2016 becoming enforceable on 25 May 2018 superseding the Data Protection Directive 95/46/EC. It imposes obligations on all organisations, anywhere in the World, who target, collect and process any personal data of all individuals who live in the EU and the European Economic Area (EEA). It also covers the transfer of personal data outside the EU and EEA areas. The primary aim of the GDPR is to give control to individuals (known as Data Subjects in the GDPR) over their personal data. As an EU Regulation, it became law in all member states of the EU (including the UK). It also applies to the EEA States.
Governing Board	A Governing Board should have a diversity of knowledge, skills and experience to enable it to be effective in providing strategic leadership and accountability in schools. It's key functions: • Overseeing the financial performance of the school making sure its money is well spent; • Holding the headteacher to account for the educational performance of the school and its pupils; • Ensuring clarity of vision, ethos and strategic decision; • Compliance with appropriate legislation and guidance from the relevant regulatory bodies.
Personal Data	As defined by the GDPR and DPA 2018, Personal Data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". This means personal data has to be information that relates to an individual. That individual must be identified or identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual. A "natural person" is a living person. Personal data includes, but is not limited to: • Contact information about pupils, staff, parents and those with parental responsibility • Health information • Details about recipients of pupil premium • Employee references • Safeguarding information about an individual • Passport information, if planning trips to the EU • Pupil exam references and results The GDPR does not cover information which is not, or is not intended to be, part of a 'filing system'. However, under the DPA 2018 unstructured manual information processed only by public authorities constitutes personal data.

	This includes paper records that are not held as part of a filing system. While such information is personal data under the DPA 2018, it is exempted from most of the principles and obligations in the GDPR and is aimed at ensuring that it is appropriately protected for requests under the Freedom of Information Act 2000.
Personal Data Breach	The school will make all reasonable endeavours to ensure there are no personal data breaches. In the unlikely event of a suspected data breach, the school will follow the procedure set out in Appendix 4. When appropriate, the data breach will be reported to the ICO within 72 hours of the school becoming aware of it. Such breaches in a school context may include, but are not limited to: • A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium; • Safeguarding information being made available to an unauthorised person; • The theft or loss of a school laptop containing non-encrypted personal data about pupils.
Special Categories of Personal Data	Some of the personal data which can be processed is more sensitive in nature and so requires a higher level of protection. These are referred to as "special categories of personal data". This means personal data about an individual's: • Race • Ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data (such as fingerprints, retina and iris patters), where this is used for identification purposes • Health data (physical or mental) • Sex life or sexual orientation Special Categories of Personal data can include information relating to criminal convictions and offences.
Processing	As defined by the ICO, processing in relation to personal data means "any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction)."

APPENDIX 2

DISCLOSING AND SHARING DATA

Share personal data:

1. Where there is an issue with a pupil or those with parental authority that puts the safety of staff at risk.
2. Where there is a need to liaise with other agencies - explicit consent will be sought for this.
3. Where the school's suppliers or contractors need data to enable the provision of services to staff and pupils eg IT companies. When doing this the school will:
    - 3.1. Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - 3.2. Establish a Data Sharing Agreement with the supplier or contractor, either in the contract or as a stand alone agreement, to ensure fair, lawful and transparent processing of any personal data shared
    - 3.3. Only share data that the supplier or contractor needs to carry out their service and information necessary to keep the individuals safe whilst the suppliers or contractors are working with the school
4. With law enforcement and government bodies where the school is legally required to do so.
5. With emergency services and local authorities to help them respond to an emergency situation that affects any of the pupils and / or staff
6. Where the personal data needs to be transferred to a country or territory outside the EEA or a country deemed Adequate by the European Commission, it will be done so in accordance with data protection law.
7. Bodies with whom personal data may be shared:
    - 7.1. Local Authority
    - 7.2. Department for Education (DfE)
    - 7.3. Other Education Providers
    - 7.4. OFSTED
    - 7.5. NHS
    - 7.6. School Nurse
    - 7.7. Health & Safety Executive
    - 7.8. Multi-Agency partners
    - 7.9. Awarding bodies
    - 7.10. Service Providers who provided learning platforms and communications tools

APPENDIX 3

RESPONDING TO SUBJECT ACCESS REQUESTS

1. Individuals can make SARs verbally or in writing including via social media;
2. In most circumstances a fee cannot be charged for dealing with a SAR;
3. The SAR should be responded to without delay and within 1 calendar month of receipt of the request;
4. If the SAR is complex or there are multiple requests from the individual, it is possible to extend the response time limit by a further two months, but the individual must be informed of the extension within the original timescale ie 1 calendar month from receipt of the SAR;
5. The information must be provided in an accessible, concise and intelligible format;
6. The information should be disclosed securely;
7. It is possible to refuse to comply with a SAR if an exemption or restriction applies or the request is manifestly unfounded or excessive.
8. When responding to requests the school:
    - 8.1. May ask the individual to provide 2 forms of identification;
    - 8.2. May contact the individual via phone to confirm the request was made;
    - 8.3. Will respond without delay and within 1 calendar month of receipt of the request;
    - 8.4. Will provide the information free of charge;
    - 8.5. May tell the individual that it may take up to 3 calendar months from receipt of the request to comply where a request is complex or numerous. The individual will be informed of this within 1 calendar month with an explanation of why the extension is required.
9. Information will not be disclosed if it:
    - 9.1. May cause serious harm to the physical or mental health of the pupil of another individual;
    - 9.2. Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
    - 9.3. Would include another individual's personal data that cannot be reasonably anonymised, the school does not have the other individual's consent and it would be unreasonable to proceed without it;
    - 9.4. Is part of certain sensitive documentation such as those related to crime, immigration legal proceedings or legal professional privilege, management forecast, negotiations, confidential references or exam scripts.
10. If the request is unfounded or excessive, the school may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
11. A request will be deemed to be unfounded or excessive if it is repetitive, or askes for further copies of the same information.
12. When a request is refused, the school will inform the individual why and tell them they have the right to lodge a complaint with the ICO.

APPENDIX 4

PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Headteacher who will contact the DPO.

1. The DPO will assist in the investigation of the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    1.1. Lost
    1.2. Stolen
    1.3. Destroyed
    1.4. Altered
    1.5. Disclosed or made available where it should not have been
    1.6. Made available to unauthorised people
2. The DPO will determine whether to alert the chair of governors.
3. The DPO will assist in making all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
4. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
5. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    5.1. Loss of control over their data;
    5.2. Discrimination;
    5.3. Identity theft or fraud;
    5.4. Financial loss;
    5.5. Unauthorised reversal of pseudonymisation (for example key-coding);
    5.6. Damage to reputation;
    5.7. Loss of confidentiality;
    5.8. Any other significant economic or social disadvantage to the individual(s) concerned.
6. If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
7. The DPO will ensure that the decision is documented (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system, or on a designated software solution.
8. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours of becoming aware of the breach. As required, the DPO will set out:
    8.1. A description of the nature of the personal data breach including, where possible:
        a The categories and approximate number of individuals concerned;
        b The categories and approximate number of personal data records concerned.
    8.2. The name and contact details of the DPO.
    8.3. A description of the likely consequences of the personal data breach.

8.4. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

9. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

10. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact and ensure that any decision on whether to contact individuals is documented. If the risk is high, the DPO, or data protection lead will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out in plain language:

    10.1. The name and contact details of the DPO;

    10.2. A description of the likely consequences of the personal data breach;

    10.3. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

11. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

12. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    12.1. Facts and cause

    12.2. Effects

    12.3. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

    Records of all breaches will be stored on the school's computer system, or on a designated software solution.

    The DPO, headteacher or designated senior leader will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

13. Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

14. Sensitive information being disclosed via email (including safeguarding records)

14.1. If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error;

14.2. Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error;

14.3. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it;

14.4. In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way;

14.5. The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request;

14.6. The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

15. Other types of breach that you might want to consider could include:

15.1. Details of pupil premium interventions for named children being published on the school website;

15.2. Non-anonymised pupil exam results or staff pay information being shared with governors;

15.3. A school laptop containing non-encrypted sensitive personal data being stolen or hacked;

15.4. The school's cashless payment provider being hacked and parents' financial details stolen.