

DATA PROTECTION POLICY

including

FREEDOM OF INFORMATION POLICY

Reviewed July 2026

Next Review due September 2027

Contents

1. Introduction
2. About this policy
3. Definition of data protection terms
4. Data Protection Officer
5. Responsibilities of the Trust/Academy/School
6. Responsibilities of Staff, Governors and Volunteers
7. Informing parents/guardians and seeking consent
8. Rights of the data subject
9. Freedom of information request policy
10. Data security
11. Data breaches
12. Data retention policy including Records Management
13. Reporting policy incidents
14. Monitoring and evaluation

Appendix 1.1 Data protection terms and definitions

Appendix 1.2 Rights of the data subject and how we uphold them

Appendix 2: Appropriate Policy Document

Appendix 3 Roles of the Data Protection Officer and Data Protection Lead

Appendix 3 Data Protection Impact Assessment

Appendix 5 Subject Access Request process

Appendix 6 Freedom of Information request process

Appendix 7 Data breach process

Manor Court Community Primary School

Data Protection Policy

Contact Information

Data Protection Officer	Amy Brittan dposchools@somerset.gov.uk
Trust Data Protection Lead	Alison Draper adraper@ppat365.org
School Data Protection Lead	Dan Glentworth office@manorcourt.ppat365.org
School Phone Number	01460 62350

Introduction

1.1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities. Manor Court Community Primary School will collect, store and process personal data about our students, workforce, parents, and others. This makes us a data controller in relation to that personal data.

1.2. We are committed to the protection of all personal data and special category personal data for which we are the data controller, and the Trust is registered as a data controller with the Information Commissioner's Office (registration number Z6486752).

1.3. The law imposes significant fines and reputational penalties for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in penalties being applied.

1.4. All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

About this policy

2.1 The types of personal data that we may be required to handle include information about students, parents, our workforce (including staff, volunteers, and governors) and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018, and other regulations (together 'Data Protection legislation').

2.2 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

Definition of data protection terms

3.1 A list of definitions is included in Appendix 1.1 to this policy.

Data Protection Officer

4.1 As a Trust we are required to appoint a Data Protection Officer (DPO - **see Appendix 3**). Our DPO is Amy Brittan and can be contacted at dposchools@somerset.gov.uk

4.2 The DPO is responsible for ensuring compliance with the Data Protection legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.3 The DPO will provide the Trust with an annual report on compliance including reported data breaches, requested for information and other interactions with the Trust

4.4 Other day to day matters will be dealt with by The Data Protection Lead (DPL - **see Appendix 3**), Headteachers, Deputy Headteachers, and Senior Administrators with the full support and guidance of the DPO.

Responsibilities of each Trust School and Central Team Member

5.1 The Trust is committed to protecting and respecting the confidentiality of sensitive information relating to staff, students, parents, and governors. The Trust will:

a) Follow the key principles of Data Protection legislation including the 6+1 principles of UK GDPR (**see Appendix 1.2**);
b) register with the Information Commissioners Office (ICO);
c) keep an up-to-date Data Asset Audit which lists all known uses of personal data in the trust including the lawful basis for processing under Data Protection legislation, who it is shared with, where it is stored (including transfer out of the UK) and how long it is retained for. Schools produce and keep a copy of their own data asset audits which are checked by the DPO
d) verify that all systems that involve personal data or confidential information will be examined to see that they meet Data Protection regulations (see **paragraph 10 Data security**)
e) inform all users about their rights regarding data protection;
f) ensure that staff complete regular data protection training including the video training provided by the DPO here https://safeshare.tv/x/czocTFK0Zv4
g) ensure that staff complete regular cyber security training including the training from the National Cyber Security Centre https://www.ncsc.gov.uk/information/cyber-security-training-schools
h) monitor its data protection and information security processes on a regular basis, changing practices if necessary (see **paragraph 10 Data security**).

Responsibilities of Staff, Directors, Governors, and Volunteers

6.1 All staff, directors, governors, and volunteers are responsible for checking that any information that they provide to the Trust or School is accurate and up to date.

6.2 Staff, directors, governors, and volunteers will complete annual data protection training as defined by the Trust by following this link

6.3 All staff, directors, governors, and volunteers are responsible for ensuring that any personal data they use in the process of completing their role:

a) is not in the view of others who do not have the authority to view the data;
b) is kept securely in a locked cabinet when not being used;
c) is stored on a secure local or network drive;
d) if on a school PC or laptop, that the device is locked when the staff member is out of the room;
e) that passwords for school systems are not shared with other staff members or students;
f) if kept on removable storage (laptop, tablet, USB memory stick) approved by the school, that this is password protected and encrypted. The data held on these devices must be backed up regularly and this is the responsibility of the individual;
g) is not disclosed to any unauthorised third party (this includes verbal disclosures of confidential information);
h) is assessed and approved by the Senior Leadership Team or the DPL with advice from the DPO (see **Appendix 4 Privacy Impact Assessment**) if used within an app, webservice or other application.

6.4 Staff, directors, governors, and volunteers should follow the security measures set out in **paragraph 10 Data security.**

6.5 Staff, directors, governors, and volunteers will report any loss, theft or mishandling of personal data promptly to the data protection lead.

6.6 Staff, directors, governors, and volunteers should note that unauthorised disclosure or transgression of the above statements or security measures in may result in disciplinary or other action.

6.7 Staff and Governors should ensure that they use the email address provided by the Trust or School for **only** school-related business and communication. All communication remains the property of the Trust and School and may be disclosed as part of a Subject Access Request (**see Appendix 5**)

6.8 If using a personal device to access school emails, the staff member / director/ governor will take care not to download any personal information about students or other staff to their personal device, and respond to emails within the email app.

6.9 Staff, Directors, and Governors will follow the email retention policy as laid out in **paragraph 12 Data retention policy including Records Management.**

6.10 When Staff, Directors and Governors leave the Trust or School, they are required to hand over all personal data belonging to other students or staff. They must not remove any personal data without the permission of the Trust or School. Taking personal data with no lawful basis may be a criminal offence.

Informing parents/guardians and seeking consent

7.1 Each school will inform the Parents/Guardians of the importance of the personal data the School uses and the importance of keeping this up to date. This process will include at least an annual data collection sheet (with the return of this document being recorded) and reminders to update personal information (e.g. contact numbers) in newsletters and at tutor or class meetings.

7.2 Consent will be sought regarding matters of non-statutory use of personal data such as the use of images and names in publicity materials on induction or when required. The returns to these permissions will be recorded and exemptions communicated to staff.

~~7.3~~ We will seek consent for each pupil from an individual with parental responsibility for that pupil. . If estranged parents cannot agree on consent, we will consider this as no consent in place, in line with guidance from the DfE https://www.gov.uk/government/publications/dealing-with-issues-relating-to-parental-responsibility/understanding-and-dealing-with-issues-relating-to-parental-responsibility#obtaining-consent

7.4 If consent is required for any other processing of personal data of any data subject, then the form of this consent must:

a. inform the data subject or their parent as appropriate, of exactly what we intend to do with their personal data
b. require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in
c. inform the data subject of how they can withdraw their consent.
d. Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

7.5 The DPO must always be consulted in relation to any consent form before consent is obtained.

7.6 A record must always be kept of any consent, including how it was obtained and when.

Rights of the data subject

8.1 All people having personal data stored by the Trust and its Schools have the right to:

a) obtain from the Trust or School confirmation if personal data concerning him or her (or their child) is being processed;
b) Where this is the case, have a copy of the personal data and the following information:

(i) the purposes of the processing;
(ii) the third parties that the data will be shared with;
(iii) the period for which the personal data will be stored;
(iv) the existence of the right to request from the Trust or School to correct, erase or restrict processing of personal data if the data can be proved to be incorrectly held;
(v) the right to lodge a complaint with a supervisory authority;
(vi) where the personal data is not collected from the data subject, any available information as to its source.

c) if exemptions are placed on any of the data above, because of safeguarding or other issues, the existence of this data will be declared.

8.2 Each school will place on its website a Privacy Notice regarding the personal data held about pupils and why it is processed. Privacy Notices for workforce, directors and governors will be distributed to data subjects and published on the Trust's website. They will be based on the DfE's privacy notices here https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices Privacy notices for recruitment are uploaded to the Trust's website.

8.3 Access to the data is called a Subject Access Request. Any person who wishes to exercise this right (or their parental right) should make a request (which does not need to be in writing) and submit it to the Headteacher or CEO. The process for dealing with a Subject Access Request is outlined in **Appendix 5**.

8.4 The Trust and its Schools aims to comply with requests for access to personal information as quickly as possible and in accordance with advice from the ICO and other professional agencies.

8.5 For further information on how the Trust upholds the rights of the data subject please see **Appendix 1.3**

Freedom of Information request policy

9.1 The Local Governing Body of Manor Court Community Primary School is committed to openness and transparency and this policy sets out the procedures and obligations on the Trust when a Freedom of Information request is received.

9.2 The Freedom of Information Act allows anyone to request information without giving a reason. The request must though state the name and address of the person as well as what information they are seeking. When a request is received this will be considered and the information, if held, will be provided unless one of the exemptions in the Act applies.

9.3 **Making requests**: Requests for information should be made clear and addressed to the Trust Data Protection Lead via the PPAT central office or headteacher of each school. The contact details of all schools can be found on their websites or by following this link The PPAT central team may be contacted on 01935 676350 or ppat@ppat365.org or by writing to PPAT Education, Kingfisher Primary School, Kingfisher Drive, Yeovil, Somerset BA22 8FJ

9.4 **Responding to requests**: Any request made to PPAT Education or its schools will be complied with in accordance with the time limits in the Act. For schools, this is 20 school days (i.e. not including weekends, holidays, or school closure days) or 60 working days if this is shorter. The Trust/school will inform the DPO of the request.

9.5 **Charges:** Manor Court Community Primary School will respond to most requests free of charge and only charge where significant costs are incurred. The school may choose to charge a fee for complying with requests for information under FOI. The fees will be calculated according to FOI regulations and the person notified of the charge before information is supplied. and its schools reserve the right to refuse to supply information where the cost of doing so exceeds the statutory maximum.

9.6 **Exemptions:** Whenever a request for information is received it will be reviewed with consideration given to whether one of the exemptions set out in the Act applies. Common exemptions include the data protection of others, confidentiality, the request going beyond the costs limit and prejudice being caused to the effective conduct of public affairs. There are other exemptions that may also be relevant. Where an exemption is being relied on to prevent disclosure of information, we would inform you that this is the case in our refusal notice.

9.7 **Publication scheme:** Manor Court Community Primary School has adopted the Information Commissioner's model publication scheme and explanatory note, stating

what information can be accessed and the process for accessing information. The publication scheme and explanatory note can be found here

9.8 **Complaints:** Anyone who has made an FOI request to the schools and who is not happy with the response that has been received can have an internal review of how their request has been handled. This will be generally carried out by a senior member of staff who was not involved in the initial request response. If a requester wishes to have an internal review, this should be requested within two months of the initial decision being communicated. Once an internal review request is received, we aim to conclude the review and communicate the outcome of this within 20 school days. Following an internal review, if the requester is still not happy with the response, they have the right to complain to the Information Commissioner's Office.

9.9 The process and record keeping for FOI requests is given in **Appendix 6**.

Data security

10.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

10.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

10.3 Security procedures include:

a. **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the Office Manager or Head Teacher.
b. **Staff network and software permissions.** Staff and those with a governance role will only have the level of permissions required for their role. When staff or someone with a governance role leave the school all their permissions and accounts will be deleted.
c. **Data walks.** The DPL and GDPR governor conduct an annual data walk to assess the risk of data loss around school, including physical security. The record of the walk and findings forms part of our monitoring documentation.
d. **Data on display.** All personal data on display has been assessed for risk and minimised where necessary. Consent has been sought for display where we do not have a legal, public interest, or legitimate interest in displaying the personal data.
e. **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind, or information which would cause distress or harm if it were disclosed. Student exercise books are not locked away as we have assessed the risk of data loss to be disproportionate to the cost of storage.

f. **Data Protection Impact Assessments.** In line with Data Protection legislation, the school carry out a -Data Protection Impact Assessment when using software or online tools which may, if breached, cause harm to the rights and freedoms of individuals. These risk assessments will be carried out with the support of the DPO (see **Appendix 4 Data Protection Impact Assessment)** The risk of data being transferred in and out of the UK will also be assessed.

g. **Methods of disposal.** Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required. IT assets are disposed of in accordance with the ICO's guidance on the disposal of IT assets.

h. **Data retention**. To minimise the risk of data being lost or mishandled, we will not retain data including emails any longer than is required by law or where there is a business need. **See paragraph 12 Data retention policy.**

i. **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their device when it is left unattended.

j. **Working away from the school premises – paper documents.** Staff are permitted to take children's work/exercise books and mark books home, ensuring that they are stored safely, e.g. when in transit, car doors to be locked if leaving vehicle. Staff are discouraged to take home documentation such as SEND reports, but on occasion this may be necessary. When necessary, such documentation should be stored securely in folders marked confidential and be stored in closed bags so it cannot be seen. e.g. through a car window. All staff are responsible for the safe handling of pupil personal data when taken off-site and any loss or disclosure to third parties must be reported to the school data protection lead as soon as possible.

k. **Working away from the school premises – electronic working**. Staff are encouraged to access electronic documents via remote secure home access. When this is not possible, the school provides encrypted data sticks to store any data. If staff are using personal devices, e.g. laptops and PCs for school business, care must be taken to ensure that family members or other third parties do not access any information relating to pupils at the school. A personal laptop or PC must have up to date virus protection. If staff believe pupil personal data may have been disclosed to third parties, this must be reported to the school data protection lead as soon as possible.

l. **Document printing.** Documents containing personal data must be collected immediately from printers and not left on photocopiers.

10.4 Specific cybersecurity measures include:

a. **In the event of a cyberattack.** Staff must follow the Trust's procedure e.g. turn off device and inform the central or school office and do not connect device to the network until it has been checked by the Trust's IT support provider. If systems are infected, the Trust and its Schools will follow the Business Continuity Plan, inform the Trust IT support provider, and Action Fraud. If personal data has been accessed, disclosed or is irretrievable, the Trust and its Schools will follow the Data Breach procedure in Section 11.

b. **Password security** Current best practice is not to make users change their passwords but to ensure they set a good strong password in the first instance.
c. **Admin password security.** The Trust and its Schools will retain all high-level login details for their systems including administrator passwords for the network, wireless connections, anti-virus, remote learning systems. The login details will be kept securely in the central or school office as appropriate
d. **Permissions.** User access to systems will be regularly reviewed by the Trust IT support provider and access will be removed or downgraded when no longer required e.g. when a user has left. All access will be reviewed annually as part of end of year tasks.
e. **Anti-virus and firewall protection**. The Trust and its Schools will have appropriate systems in place to protect against cyberattack, ransomware and compromised accounts. This will be annually checked by the Trust IT support provider
f. **Encryption.** All devices that have access to data attached to the network are fully encrypted in line with current guidance from Schools ICT at Somerset Council.
g. **Personal devices.** Personal devices may connect to the network with SLT permission but in full compliance with the ICT policies and this permission may be withdrawn at any time. The Trust's technical support will inform the owner/user that if a mobile device connects to the internet connection, then the device's online activity will be monitored and logged by the Trust's Internet Service Provider.
h. **Back-ups.** Information including data in SIMS and the school network drives is backed up remotely at regular intervals determined by the trust's technical support. The trust's IT support provider will carry out annual testing of the back-ups to ensure that information can be restored in the event of the systems being compromised.
i. **Staff cybersecurity training.** Staff, Directors and Governors will complete the National Cyber Security Centre's Training for School Staff https://www.ncsc.gov.uk/information/cyber-security-training-schools to increase awareness of possible risk. This will be part of induction for new staff and a requirement for existing staff.
j. **Acceptable User Policies.** Staff, Directors, Governors, Volunteers and learners, and the Trust's IT technical support provider will sign and follow the Trust's appropriate Acceptable Use Policies.

10.5 Any member of staff found to be in breach of the security measures may be subject to disciplinary action.

Data breaches

11.1 If there is a data breach the School will inform the DPO who will then advise on any actions.

11.2 Any data breaches will be recorded, comprising the facts relating to the personal data breach, its effects and the remedial action taken as shown in Appendix 7.

11.3 If there is judged to be a significant risk to the rights and freedoms of the affected data subject, the School will communicate the breach to the data subjects with the support of the DPO.

11.4 In the case of a personal data breach where there is a significant risk of harm to the rights and freedoms of data subjects, the ICO should be informed as soon as possible and **within 72 hours of notification**. Further investigation of the breach can take place after this notification in line with advice from the DPO and the ICO.

11.5 When reporting a breach, Data Protection legislation states that we must provide:

a. a description of the nature of the personal data breach including, where possible:
b. the categories and approximate number of individuals concerned; and
c. the categories and approximate number of personal data records concerned;
d. the name and contact details of the data protection officer or other contact point where more information can be obtained;
e. a description of the likely consequences of the personal data breach; and
f. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects, and to minimise risk of a repeated incident.

Data retention policy including Records Management

12.1 The Trust has a comprehensive scheme for records management which is made up of policies, procedures, systems, processes, and behaviours.

12.2 Our scheme ensures that we have reliable evidence of our actions and decisions which is available for reference and use when needed. This supports us to comply with the Accountability Principle of UK GDPR.

12.3 Our Records Management is overseen by the following staff: the CFO, Headteachers, Office Managers and the Data Protection Officer. The CEO and CFO will be advised of any issues at any school.

Our scheme includes the following:

a. **Data Protection and Freedom of Information Policy**: this explains our legal responsibilities as a data controller; how staff will process records securely; how we have technical and physical security in place; how we manage access to records; how we manage data loss or mismanagement; and how long we keep data for.

b. **Data Asset Audit (Record of Processing Activities):** this is a statutory document (to comply with Article 30 of UK GDPR) and lists all the data we process in school, where it is, who it is shared with, our lawful basis for processing, and our retention schedule. Schools produce and keep a copy of their own data asset audits which are checked by the DPO

c. **Data Protection Officer**: our Data Protection Officer provides strategic advice and supports the school to comply with statutory legislation including effective records management and monitors the school's compliance through audits and an annual report.

d. **Retention Schedule**: we follow guidance from Somerset Local Authority on records retention, to ensure that we are compliant with legislation, including Keeping Children Safe in Education, and any over-riding current legal holds on data destruction. We also follow the 2019 Information and Records Management Society's Schools Records Management Toolkit for schools http://irms.org.uk/page/SchoolsToolkit

e. **Privacy Notices:** these explain to data subjects how we will keep their records in a way that is compliant with the law.

f. **Data breach log:** we have a record of incidents of personal data loss or disclosure. Individual logs are kept by each school and by the central team

g. **Subject Access / Freedom of Information request log:** we have a record of any request for information relating to records held by the school. Individual logs are kept by each school and by the central team

h. **Staff training:** our staff receive induction and update training on how to keep personal data and records safe and have completed the National Cyber Security Centre training on cyber risks, which may affect the integrity and security of our records.

i. **Acceptable User Policies**: all staff, directors, governors and parents (on behalf of pupils) sign an acceptable user agreement which states how they will use technology in school including how they will access records held on the server or other systems such as SIMS.

j. **Technical security systems**: we contract with an external company, Praestantia, that ensures that our firewall and anti-virus systems are up to date; that records are backed up and retrievable; that threats to our systems are identified and addressed.

k. **Management Information System support**: the Trust procures support from the School ICT Support Service to ensure that our system is up to date, secure and compliant.

l. **Destruction of confidential waste**: Some schools have a contract with a contractor to remove confidential data waste from the school and dispose of it securely otherwise schools and the central team have confidential waste sacks in the office for the shredding of sensitive and Special Category personal data.

m. **Secure destruction of hardware**: we retain certificates of secure data destruction from third party contractors with appropriate professional accreditation when hardware is removed from the school e.g. photocopiers, computers, or devices.

n. **Emails**: the Trust has a clear email retention policy of 730 days. Emails containing personal information of students or staff members which may be required for learning or safeguarding purposes are attached to the student or staff members SIMS or CPOMS / My Concern / Safeguarding folder and permanently deleted from our email system.

Reporting policy incidents

13.1 Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data in a school should raise the matter with the Head Teacher or the Chair of Governors if it is the Head who has not followed the policy. Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data in the central team should raise the matter with the CEO or the Chair of the Trust Board

Monitoring and evaluation

14.1 This policy will be monitored and reviewed in line with the Trust's policy review procedure.

14.2 The Trust will monitor the implementation of the policy through annual data protection walks around the Trust's sites to ensure that the Trust's requirements are followed by staff. These walks will be conducted by the on-site Data Protection Lead and a governor or director.

Appendix 1.1: Data Protection terms and definitions

Term	Definition
Data	Information, which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Asset Audit/ Record of Processing Activities (ROPA)	The inventory of all the data processed by the Trust and its Schools including the lawful basis for processing, who it is shared with, where it is transferred (including out of the UK) and how long it is retained for,
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes students, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	Any information relating to an identified or identifiable living natural person (a data subject); an identifiable living 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.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	Those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

Appendix 1.2: Rights of the data subject and how we uphold them

1. **The right to be informed:** Data subjects are informed of how we process their personal data through Privacy Notices.

2. **The right of access:** Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the school's Subject Access Request Procedure.

3. **The right to rectification:** If a data subject informs the Trust that personal data held about them by the Trust is inaccurate or incomplete then we will consider that request and provide a response within one month. If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case. We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the ICO (Information Commissioners Office) at the time that we inform them of our decision in relation to their request.

4. **The right to erasure**: Data subjects have a right to have personal data about them held by the Trust or School erased only in the following circumstances.
   - Where the personal data is no longer necessary for the purpose for which it was originally collected.
   - When a data subject withdraws consent – which will apply only where the Trust or School is relying on the individuals consent to the processing in the first place.
   - When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object.
   - Where the processing of the personal data is otherwise unlawful.
   - When it is necessary to erase the personal data to comply with a legal obligation.
   - If the Trust or School offers information society services to a pupil and consent is withdrawn in respect of that pupil in relation to those services.

   The Trust is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:
   - to exercise the right of freedom of expression or information
   - to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
   - for public health purposes in the public interest
   - for archiving purposes in the public interest, research, or statistical purposes
   - in relation to a legal claim.

   If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible

or involves a disproportionate effort. The DPO must be consulted in relation to requests under this right.

5. **The right to restrict processing**: Data subjects have a right to 'block' or suppress the processing of personal data. This means that the Trust ~~or School~~ can continue to hold the personal data but not do anything else with it.
   The Trust or School must restrict the processing of personal data:
   - where it is in the process of considering a request for personal data to be rectified (see above)
   - where the Trust is in the process of considering an objection to processing by a data subject
   - where the processing is unlawful, but the data subject has asked the Trust not to delete the personal data
   - where the Trust no longer needs the personal data, but the data subject has asked Trust or School not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the Trust
   - If the Trust has shared the relevant personal data with any other organisation, then we will contact those organisations to inform them of any restriction unless this proves impossible or involves a disproportionate effort.

   The DPO must be consulted in relation to requests under this right.

6. **The right to data portability**: In limited circumstances a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to another organisation. If such a request is made, then the DPO must be consulted.

7. **The right to object**: In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest. An objection to processing does not have to be complied with where Trust or School can demonstrate compelling legitimate grounds which override the rights of the data subject. Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right. In respect of direct marketing any objection to processing must be complied with. The Trust is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

8. **Rights in relation to automated decision making and profiling:** The Trust will carefully consider whether it takes any decisions about any individuals by automated means. This includes any decisions made solely by automated means, and which has a legal effect in relation to the individual. This might include, for example, a decision as to whether to employ an individual. We consider it to be unlikely that this would apply to a Trust as there is always likely to be an element of human intervention in any decision making. However careful consideration should be given to this issue.

Appendix 2: Appropriate Policy Document

1. Scope

The Data Protection Act 2018 outlines the requirement for an appropriate policy document to be in place when processing special category and criminal offence data under certain specified conditions.

In order to operate effectively, the Trust and its schools have to process personal information which is listed in Schedule 1 of the Data Protection Act 2018. Almost all of the conditions in Schedule 1 of the Data Protection Act 2018, require an Appropriate Policy Document in place.

The Trust is committed to demonstrating that its processing of Schedule 1 conditions is compliant with the requirements of the UK General Data Protection Regulation (UK GDPR) Article 5 principles. This Appropriate Policy Document therefore complements the school's record of processing under Article 30 of the UK GDPR and provides special category and criminal offence data with further protection and accountability.

2. Description of processing which requires an appropriate policy document

Schedule 1, Part 1 – Conditions relating to employment, social security, and social protection.

- Employment, social security, and social protection
- Processing personal data concerning health in connection with our rights under employment law.
- Processing data relating to criminal convictions under Article 10 UK GDPR in connection with our rights under employment law in connection with recruitment, discipline, or dismissal.

Schedule 1, Part 2 – Substantial Public Interest Conditions

Statutory etc. and government purposes

- Fulfilling the Trust's obligations under UK legislation for the provision of education to school aged children
- Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.
- We may also process criminal offence data under this condition.

Equality of opportunity or treatment

- Ensuring compliance with the school's obligations under legislation such as the Equality Act 2010.
- Ensuring that we fulfil our public sector equality duty when carrying out our work.

- Ensuring we provide equal access to our services, to all pupils in recognition of our legal and ethical duty to represent and serve pupils.

Preventing or detecting unlawful acts

- Processing data concerning criminal records in connection with employment in order to reduce the risk to the school and safeguard pupils and the wider community.
- Disclosing data to support the prevention or detection of unlawful acts.

Protecting the public against dishonesty etc.

- Processing data concerning dishonesty, malpractice, or other improper conduct in order to safeguard and protect pupils and the wider community.
- Carrying out investigations and disciplinary actions relating to our employees.
- Regulatory requirements relating to unlawful acts and dishonesty etc.
- Assisting other agencies in connection with their regulatory requirements.

Support for individuals with a particular disability or medical condition

- To provide services or raise awareness of a disability or medical condition in order to deliver services to individuals.

Counselling

- For the provision of confidential counselling organised through Occupational Health, advice, or support or of another similar service provided confidentially.

Safeguarding of children and individuals at risk

- Protecting vulnerable children and young people from neglect, physical, mental, or emotional harm.
- Identifying individuals at risk while attending emergency incidents.
- Obtaining further support for children and individuals at risk by sharing information with relevant agencies.

Insurance

- Information that is necessary for insurance purposes.

Occupational pensions

- Fulfilling the Trust's obligation to provide an occupational pension scheme.

Schedule 1, Part 3 – Additional Conditions Relating to Criminal Convictions, etc.

- The Trust may process personal data relating to criminal convictions in connection with its service obligations or as part of recruitment and employment checks to safeguard and protect pupils and the wider community against dishonesty.

3. Data Protection Principles

Article 5 of the UK GDPR states that personal data shall be:

- Processed lawfully, fairly, and transparently
- Collected for specific and legitimate purposes and processed in accordance with those purposes
- Adequate, relevant, and limited to what is necessary for the stated purposes
- Accurate and, where necessary, kept up-to-date
- Retained for no longer than necessary, and
- Kept secure

In addition, Article 5 requires that the data controller shall be responsible for, and able to demonstrate compliance with, these principles (the accountability principle).

Processed lawfully, fairly, and transparently

- The Trust provides clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices and policy documents.
- Our processing for purposes of substantial public interest is necessary to exercise our functions which are outlined in legislation.
- Our processing for the purposes of employment relates to our obligations as an employer.
- We also process special category personal data to comply with other obligations imposed on the school in its capacity as an educational institute e.g. the Equality Act.
- The Senior Leadership Team, Directors and Governors oversees policy work and monitors compliance in all areas of Information Governance, as outlined in its terms of reference.
- We carry out data protection impact assessments to ensure processing is fair and lawful.

Collected for specific, explicit, and legitimate purposes

- We process personal data for purposes of substantial public interest as explained above when the processing is necessary for us to fulfil our statutory functions, where it is necessary for complying with or assisting another to comply with a regulatory requirement, to establish whether an unlawful or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts or for disclosure to elected representatives.
- We are authorised by law to process personal data for the purposes outlined above.
- We process personal data only when it is necessary and proportionate.
- If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.
- We will not process personal data for purposes incompatible with the original purpose it was collected for. If we do use personal data for a new purpose that is compatible, we will inform the data subject first.

Adequate, relevant, and limited to what is necessary for processing

- We collect personal data necessary for the relevant purposes and ensure it is not excessive.
- The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Accurate and kept up to date with every effort to erase or rectify without delay

- Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. The Trust and its Schools have processes in place to help people do this.
- If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision.

Kept in a form such that the data subject can be identified only as long as is necessary for processing.

- All data processed by the Trust and its Schools unless retained longer for archiving purposes, will be retained for the periods set out in our retention schedules. The requirement for retention schedules is outlined in our Records Management and Data Quality Policy.
- We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs.
- Our retention schedule is reviewed regularly and updated when necessary.
- We anonymise data when possible.

Processed in a manner that ensures the appropriate security

- The Trust will carry out risk assessments taking into account state of the art technical measures, the costs of implementation and the risk/likelihood to individuals if a security breach occurs and the effect of any security breach on the Trust or School itself.
- Both the Trust and its processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- When assessing appropriate organisational and technical measures, the School Data Protection Lead and Head Teacher will consult with other relevant parties, such as the Trust's IT provider, the Chief Finance Officer & the Trust Data Protection Lead.
- Our Senior Leadership Team, Directors and Governors meet regularly to ensure suitable information security governance is deployed throughout the Trust and its Schools
- Employees working within the Trust and its Schools and those with a governance role are to undertake a Disclosure and Barring Service (DBS) check.

- All of our staff are trained in data protection matters and our contracts include confidentiality clauses.
- Technical security controls such as encryption are employed to secure sensitive information within systems.
- Role-based access controls are implemented to restrict access to sensitive data.
- Where possible, anonymisation or pseudonymisation are used to reduce the risk of sensitive data being compromised.

Accountability principle

- The appointment of a Data Protection Officer.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.
- We have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high-risk processing.
- Regularly reviewing our accountability measures and update or amend them when required.
- The Senior Leadership Team and Directors are responsible for ensuring that the Trust is compliant with Information Governance duties.
- All staff are routinely trained in key areas, including data protection.

4. Additional special category processing

The Trust process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices.

5. Evaluation

The appropriate policy document will be subject to an annual review to ensure that it matches service delivery and the information being processed by the school.

Appendix 3: Roles of the Data Protection Officer and Data Protection Lead

Purpose

The Data Protection Officer (DPO) is responsible for monitoring compliance with current data protection law, and has the knowledge, support, and authority to do so effectively. They oversee and verify the Trust's data protection processes and advise the Trust on best practice.

The Trust Data Protection Lead (TDPL) maintains contact with the DPO (Data Protection Officer) and is responsible for assisting in monitoring with compliance and verifies the Trust's data protection practices on a day to day basis.

Within each school there will be a Data Protection Lead (DPL), who maintains contact with the TDPL and is responsible for assisting in monitoring with compliance and verifies the school's data protection practices on a day to day basis.

Data Protection Officer Responsibilities To:

- advise the Trust about their obligations under the UK General Data Protection Regulation and the Data Protection Act 2018;
- support the DPL in developing a joint understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the TDPL, with the monitoring of the Trust's compliance with data protection law, by:
    - collecting information to identify data processing activities;
    - analysing and checking the compliance of data processing activities;
    - informing, advising, and issuing recommendations to the school;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the TDPL in making sure that the Trust's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - coordinating staff training;
    - conducting internal data protection audits;
- advise on and assist the Trust with carrying out data protection impact assessments, if necessary;
- act as a contact point for the ICO, assisting and consulting it where necessary, including:
    - helping the ICO to access documents and information;

    - seeking advice on data protection issues;
- act as a contact point for individuals whose data is processed (for example, staff, students, and parents), including:
    - responding with support from the TDPL to subject access requests;
    - responding with support from the TDPL to other requests regarding individuals' rights over their data and how it is used;
- take a risk-based approach to data protection, including:
    - prioritising the higher-risk areas of data protection and focusing mostly on these
    - advising the Trust if/when it should conduct an audit, which areas staff need training in, and what the DPO/TDPL/DPL roles should involve.
- report to the board of Directors on the school's data protection compliance and associated risks;
- respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role;
- assist the TDPL in maintaining a record of the Trust's data processing activities;
- work with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the TDPL in fostering a culture of data protection throughout the Trust;
- work closely with other departments and services to ensure UK GDPR compliance, such as HR, legal, IT and security;
- work with the Senior Leadership team at the Trust to ensure UK GDPR compliance;
- assist with any additional tasks necessary to keep the Trust compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- providing a model Data Protection Policy and assist in customising it for the Trust;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- providing advice on other associated policies and documents;
- providing materials and advice in completing a dynamic Data Asset Audit// Record of Processing Activities (ROPA) and assisting in its completion if necessary;
- checking issues with the Data Asset Audit/ Record of Processing Activities (ROPA);
- providing training materials to allow the DPL to assist staff in keeping up to date with Data Protection issues;
- acting as the point of contact for SAR and FOI requests and supporting the school to provide the information as required;

- providing a Data Protection Audit on a 3 yearly rota basis and producing a report for Directors at cost;
- providing telephone and email advice and support;
- providing regional training for the TDPL and other staff;
- providing Trustbased on-demand training at cost.

Trust Data Protection Lead Responsibilities

To:

- verify that the Trust has registered with the ICO;
- support the DPO in advising the Trust about their obligations under the Data Protection Act 2018;
- support the DPO in developing an understanding of the Trust's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the DPO, with the monitoring of the Trust's compliance with data protection law, by:
    - collecting information to identify data processing activities;
    - analysing and checking the compliance of data processing activities;
    - informing, advising, and issuing recommendations to the school;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the DPO in making sure that the Trust's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - coordinating staff training;
    - conducting internal data protection audits;
- act as a contact point for the DPO in supporting individuals whose data is processed (for example, staff, students, and parents), including:
    - responding with support from the DPO to subject access requests;
    - responding with support from the DPO to other requests regarding individuals' rights over their data and how it is used;
- assist the DPO in maintaining a record of the Trust's data processing activities providing this on a yearly basis to the DPO;
- assisting the DPO in working with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPO in fostering a culture of data protection throughout the Trust;
- report to the board of Directors on the Trust's data protection compliance and associated risks;

- work with the Senior Leadership team at the Trust to ensure UK GDPR compliance;
- assist with any additional tasks necessary to keep the Trust compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- act as the point of contact with the DPO;
- assist in customising the Data Protection Policy for the Trust;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- provide advice on other associated policies and documents;
- providing materials and advice in completing a Data Asset Audit and assisting in its completion if necessary;
- supplying the DPO with the Data Asset Audit on a yearly basis;
- using the training materials provided by the DPO to assist the staff in keeping up to date with Data Protection issues.

School Data Protection Lead Responsibilities

To:

- support the DPO and TDPL in advising the school about their obligations under the Data Protection Act 2018;
- support the TDPL in developing an understanding of the Trust's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the TDPL, with the monitoring of the school's compliance with data protection law, by:
    - collecting information to identify data processing activities;
    - analysing and checking the compliance of data processing activities;
    - informing, advising and issuing recommendations to the school;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the TDPL in making sure that the Trust's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - coordinating staff training;
    - conducting internal data protection audits;
- act as a contact point for the DPO and TDPL in supporting individuals whose data is processed (for example, staff, students and parents), including:

    - responding with support from the DPO and TDPL to subject access requests;
    - responding with support from the DPO and TDPL to other requests regarding individuals' rights over their data and how it is used;
- assist the DPO and TDPL in maintaining a record of the school's data processing activities providing this on a yearly basis to the DPO/TDPL;
- assisting the DPO and TDPL in working with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the TDPL in fostering a culture of data protection throughout the school;
- work with the Senior Leadership team at the school to ensure UK GDPR compliance;
- assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- act as the point of contact with the DPO and TDPL;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- provide advice on other associated policies and documents;
- providing materials and advice in completing the Data Asset Audit / Record of Processing Activities (ROPA) and assisting in its completion if necessary;
- supplying the DPO with the Data Asset Audit / Record of Processing Activities (ROPA) on a yearly basis;
- using the training materials provided by the DPO to assist the staff in keeping up to date with Data Protection issues.

Appendix 4: Data Protection Impact Assessment

Before the use of any new service that uses personal data, staff should complete a Data Protection Assessment Form.

The Senior Leaders and/or the TDPL and SDPL, with advice from the DPO will then approve the use and the information be placed on the Data Asset Audit.

The Trust will contact the DPO for a template Data Protection Impact Assessment which will assess the risks of the project and identify actions that can minimise the risks.

The Trust will follow the guidance from the Information Commissioner's Office here https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/

Appendix 5: Subject Access Request process

On receiving a Subject Access Request or request for change or deletion of data the DPO or TDPL will:

- inform the DPL in the school (and the Headteacher if necessary);
- contact the DPO if clarity on the request is needed or procedure is needed;
- record the details of the request, updating this record where necessary
- conduct identity checks of the requester if required
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **1 calendar month**, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

Appendix 6: Freedom of Information request process

On receiving a Freedom of Information Request, which must be made in writing, the DPO, TDPL or the school will:

- inform the DPL in the school (and the Headteacher if necessary);
- contact the DPO for clarity on the request and procedure, and a sample response
- record the details of the request, updating this record where necessary
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- decide that if the material is already published or falls within an exemption;
- if data is not going to be published inform the requestor why this is not being released;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **20 school days** (i.e. not including weekends, holidays, or school closure days) or **60 working days** if this is shorter.

Appendix 7: Data breach process

Every Data Protection Breach should be recorded. The process that should be followed is listed below:

- inform the TDPL (and the CEO if necessary);
- inform the DPL in the school (and the Headteacher if necessary);

- record the details of the breach providing these details:
    - a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
    - the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
    - a description of the likely consequences of the personal data breach; and
    - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

- contact the DPO if clarity on reporting the breach is needed and if necessary, report to the ICO;

    - By phoning 0303 123 1113
    - By downloading a form from the ICO website https://cy.ico.org.uk/media/report-a-concern/forms/4019685/report-a-personal-data-breach-form.doc and emailing to icocasework@ico.org.uk
    - By filling in the online form at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/report-a-data-breach-online-form/report-a-personal-data-breach-online-form/ and sending it to casework@ico.org.uk

- updating this record where necessary;

- identify the people whose data is accidentally released, inform them of the breach and the processes taken to rectify the situation;

- review why the breach took place and if future similar events can be avoided.