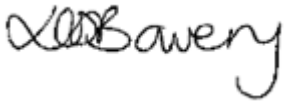
MERRIOTT & HASELBURY PLUCKNETT
PRIMARY SCHOOLS FEDERATION

Data Protection Policy

(Learning and Growing Together)

Date ratified by Governing Body	**22nd January 2024**
Review Cycle	**Every year, or when there is a change in statutory guidance or legislation**
Review Date	**January 2025**
Signed Headteacher	
Signed COG	

1. Introduction

a. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a Federation of schools, we 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.

b. We are committed to the protection of all personal data and special category personal data for which we are the data controller.

c. 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.

d. 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.

e. Within this policy, 'the school' relates to both schools within the Federation of Merriott and Haselbury Plucknett Primary Schools.

2. About this Policy

a. 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 United Kingdom General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018, and other regulations (together 'Data Protection legislation').

b. 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.

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

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

3. Definition of Data Protection Terms. A list of definitions is included in Annex A to this policy.

4. Data Protection Officer

a. As a school, we are required to appoint a Data Protection Officer (DPO - see Annex D). Our DPO can be contacted at dposchools@somerset.gov.uk

b. 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.

c. Other day to day matters will be dealt with by The Data Protection Lead (DPL – see Annex E), The Headteacher, SLT, and the Administrators on each school site with the full support and guidance of the DPO.

5. Responsibilities of the School

a. The school is committed to protecting and respecting the confidentiality of sensitive information relating to staff, students, parents and governors. The school will:
   - i) Follow the key principles of Data Protection legislation including the 7 principles of UK GDPR (see Annex B);
   - ii) register with the Information Commissioners Office (ICO);
   - iii) keep an up-to-date Data Asset Audit which lists all known uses of personal data in the school, 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.
   - iv) verify that all systems that involve personal data or confidential information will be examined to see that they meet Data Protection regulations (see section 11 Data Security).
   - v) inform all users about their rights regarding data protection;
   - vi) provide training to ensure that staff know their responsibilities, monitor its data protection and information security processes on a regular basis, changing practices if necessary (see section 11 Data Security).

6. Responsibilities of Staff, Governors and Volunteers

a. All staff, governors and volunteers are responsible for checking that any information that they provide to the school is accurate and up to date.

b. All staff are responsible for ensuring that any personal data they use in the process of completing their role:
   - i) is not in the view of others who do not have the authority to view the data.
   - ii) is kept securely in a locked cabinet when not being used.
   - iii) is stored on a secure local or network drive.
   - iv) if on a school PC or laptop, that the device is locked when the staff member is out of the room.
   - v) that passwords for school systems are not shared with other staff members or students.
   - vi) 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.
   - vii) is not disclosed to any unauthorised third party (this includes verbal disclosures of confidential information).

viii) is assessed and approved by the Senior Leadership Team / DPL with advice from the DPO (see Annex F Privacy Impact Assessment) if used within an app, webservice or other application.

c. Staff should follow the security measures set out in section 11 Data Security.

d. Staff will report any loss, theft or mishandling of personal data promptly to the data protection lead.

e. Staff should note that unauthorised disclosure or transgression of the above statements or security measures in may result in disciplinary or other action.

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

g. Staff and Governors will follow the email retention policy as laid out in section 13 Data retention policy including emails.

h. When Staff and Governors leave the 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 school. Taking personal data with no lawful basis may be a criminal offence.

i. If using a personal device to access school emails, the staff member / 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.

7. Informing Parents / Guardians and Seeking Consent

a. The 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 class meetings.

b. 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.

c. In relation to all students at our school, we will seek consent from an individual with parental responsibility for that student.

d. If consent is required for any other processing of personal data of any data subject, then the form of this consent must:
   i) inform the data subject of exactly what we intend to do with their personal data.

ii) require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in.
iii) inform the data subject of how they can withdraw their consent.
iv) 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.

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

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

8. Rights of the Data Subject

a. All people having personal data stored by the school, have the right to:
i) obtain from the school confirmation if personal data concerning him or her (or their child) is being processed.
ii) Where this is the case, have a copy of the personal data and the following information;
a) the purposes of the processing.
b) the third parties that the data will be shared with.
c) the period for which the personal data will be stored.
d) the existence of the right to request from the school to correct, erase or restrict processing of personal data if the data can be proved to be incorrectly held.
e) the right to lodge a complaint with a supervisory authority.
f) where the personal data is not collected from the data subject, any available information as to its source.

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

c. The school will place on its website a Privacy Notice regarding the personal data held about students and why it is processed. Privacy Notices for workforce and governors will be distributed to data subjects by email and be held on the school website.

d. 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 Data Protection Lead. The process for dealing with a Subject Access Request is outlined in Annex G.

e. The school 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.

f. A parent or carer can request to see their child's educational record, or request it on behalf of their child, in writing. The information will be presented within 15 school days of the request. If there is a cost of retrieving the information, for example if a copy must be made, the governing body may charge the parent the amount that it will cost but no more (dependent on the number of pages of information to be supplied). Other than this, there will be no charge for the information requested.

g. For further information on how the school upholds the rights of the data subject please see Annex C.

9. Freedom of Information Request Policy

a. The governing body of the Merriott and Haselbury Plucknett Primary Schools Federation is committed to openness and transparency and this policy sets out the procedures and obligations on the school when a Freedom of Information request is received.

b. 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.

c. **Making requests**: Requests for information should be made clear and addressed to the School Data Protection Lead at either:
office@merriottprimary.co.uk
office@haselburypluckettschool.co.uk

d. **Responding to requests**: Any request made to the school 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 school will inform the DPO of the request.

e. **Charges:** The 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. The school reserve the right to refuse to supply information where the cost of doing so exceeds the statutory maximum.

f. **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.

g. **Publication scheme:** The school has adopted the Information Commissioners' model publication scheme. To sit alongside this, the school has a guide to information document which sets out what information the school will make available and how it can be accessed. This Guide can be accessed on our websites.

h. **Complaints:** Anyone who has made an FOI request to the school 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 complaint to the Information Commissioner's Office.

i. The process and record keeping for FOI requests is given in Annex H.

10. Data Security

a. 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.

b. 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.

c. Security procedures include:
   i) Entry controls**.** Any stranger seen in entry-controlled areas should be reported to a member of the senior leadership team.
   ii) Staff network and software permissions**.** Staff will only have the level of permissions required for their role. When staff leave the school, all their permissions and accounts will be deleted.
   iii) Data walks**.** The DPL and governor conduct an annual data walk to assess the risk of data loss around the school, including physical security. The record of the walk and findings forms part of our monitoring documentation.
   iv) 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.
   v) 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 was 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.

vi) Privacy Impact Assessments**.** In line with Data Protection legislation, the school will carry out a Privacy 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 Annex F Privacy Impact Assessment**)** The risk of data being transferred in and out of the UK will also be assessed.

vii) 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.

viii) 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 section 13 Data retention policy.

ix) 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.

x) Working away from the school premises – paper documents. Staff are permitted to take children's work/exercise books and markbooks 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 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.

xi) Working away from the school premises – electronic working. Staff are encouraged to access electronic documents via OneDrive or the Federation Sharepoint portal. When this is not possible, the school provide 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.

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

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

11. Specific cybersecurity measures

a. **In the event of a cyberattack.** Staff must follow the school's procedure: turn off device and inform the school office and do not connect device to the school network until it has been checked by the school technician. If systems are infected, the school will follow the Business Continuity Plan and inform the

school's technician and Action Fraud. If personal data has been accessed, disclosed or is irretrievable, the school will follow the Data Breach procedure in Section 13.

b. **Password security.** Staff are prompted to change network passwords every 30 days and passwords must be complex and not repeated. Staff will be reminded to change their email passwords annually, particularly if they have never changed their password since their account has been created. Passwords will not be shared with any other user.

c. **Admin password security.** The school 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 school office.

d. **Permissions.** User access to systems will be regularly reviewed by the school technician and access will be removed or downgraded when no longer required e.g., when a user has left the school. All access will be reviewed annually as part of end of year tasks.

e. **Anti-virus and firewall protection**. The school will have appropriate systems in place to protect against cyberattack, ransomware and compromised accounts. This will be annually checked by the school technician.

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 County 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 school'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 School's Internet Service Provider.

h. **Back-ups.** Information including data in SIMS and the school network drives is backed up onsite at regular intervals determined by the school's technical support. The school technician 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 will complete the National Cyber Security Centre's online training module 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 and learners will sign and follow the school's appropriate Acceptable Use Policies. The school's technical support will sign and

follow the specific AUP for technicians.

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

12. Data Breaches

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

b. 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 Annex I.

c. 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.

d. 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.

e. Data breaches are reported using the information found at on the ICO website https://ico.org.uk/for-organisations/report-a-breach/ and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

f. When reporting a breach, Data Protection legislation states that we must provide a description of the nature of the personal data breach including, where possible:
   i) the categories and approximate number of individuals concerned.
   ii) the categories and approximate number of personal data records concerned.
   iii) the name and contact details of the data protection officer or other contact point where more information can be obtained.
   iv) a description of the likely consequences of the personal data breach.
   v) 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.

13. Data Retention Policy including Records Management

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

b. 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.

c. Our Records Management is overseen by the following staff: the Headteacher, Finance and Operations Manager; the Data Protection Officer.

d. Our scheme includes the following:

i) **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.

ii) **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.

iii) **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.

iv) **Retention Schedule**: we follow guidance from Somerset Local Authority on records retention, to ensure that we are compliant with legislation and any over-riding current legal holds on data destruction e.g. the Independent Inquiry into Child Sexual Abuse. We also follow the Information and Records Management Society's Schools Records Management Toolkit for schools http://irms.org.uk/page/SchoolsToolkit

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

vi) **Data breach log:** we have a record of incidents of personal data loss or disclosure.

vii) **Subject Access / Freedom of Information request log:** we have a record of any request for information relating to records held by the school.

viii) **Staff training:** our staff receive induction and update training on how to keep personal data and records safe.

ix) **Acceptable User Policies**: all staff 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.

x) **Technical security systems**: we have an external technician who 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.

xi) **Management Information System support**: the school procures support from the SSE MIS Support Service to ensure that our system is up to date, secure and compliant.

xii) **Destruction of confidential waste**: The Federation uses Bowers services to remove confidential data waste from both schools and dispose of it securely. Confidential waste sacks are used in the office for the shredding of sensitive and Special Category personal data.

xiii) **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.

xiv) **Emails**: The Federation has a clear email retention policy where e-mails are deleted when no longer required, and / or when staff or students leave the school. 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.

14. Reporting Policy Incidents Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data should raise the matter with the Headteacher or Chair of Governors.

15. Monitoring and Evaluation. This policy will be monitored by the Leadership team and Governing Body.

Annexes:

A. Data Protection Terms and Definitions
B. Data Protection Principles
C. Right of the Data Subject and How We Uphold Them
D. Appropriate Policy Document
E. Role of the Data processing Officer
F. Role of the Data Protection Lead
G. Privacy Impact Assessment
H. Subject Access Request Process
I. Freedom of Information Request Process
J. Date Breach Process
K. CCTV Policy

Annex A to
Data Protection Policy

DATA PROTECTION TERMS AND CONDITIONS

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Asset Audit	The inventory of all the data processed by the school 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 data.

Annex B to
Data Protection Policy

DATA PROTECTION PRINCIPLES

1. Anyone processing personal data must comply with the 7 data protection principles, listed in Article 5 of UK GDPR.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

2. The principles are:

   a. **Lawfulness, fairness and transparency**: we have a lawful reason for collecting personal data; we process data in a way that data subjects would consider fair; and we inform all data subjects about what we're collecting.

   b. **Purpose limitation**: we only use the data for specific purposes.

   c. **Data minimisation**: we only collect and share the data we need.

   d. **Accuracy**: we make sure that the data is accurate (or make reasonable and proportionate efforts to do this).

   e. **Storage limitation**: we don't keep data longer than is necessary.

   f. **Integrity and confidentiality (security)**: we keep data safe.

   g. **Accountability**: we must have evidence to show that we have complied with the principles above.

3. Personal data must also:

   a. be processed in line with **data subjects' rights**

   b. not be transferred to people or organisations situated in other countries without adequate protection.

   c. At Merriott and Haselbury Plucknett Schools Federation we do not use or store any biometric information / data on staff or pupils.

Annex C to
Data Protection Policy

RIGHTS OF THE DATA SUBJECT AND HOW THEY ARE UPHELD

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 school that personal data held about them by the school 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 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 school erased only in the following circumstances:

a. Where the personal data is no longer necessary for the purpose for which it was originally collected.

b. When a data subject withdraws consent – which will apply only where the school is relying on the individuals consent to the processing in the first place.

c. 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.

d. Where the processing of the personal data is otherwise unlawful.

e. When it is necessary to erase the personal data to comply with a legal obligation.

f. If the school offers information society services to a pupil and consent is withdrawn in respect of that pupil in relation to those services.

g. The school is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:
   i) to exercise the right of freedom of expression or information.
   ii) to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law.

iii) for public health purposes in the public interest.
iv) for archiving purposes in the public interest, research or statistical purposes.
v) in relation to a legal claim.

h. If the school 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.

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

5. The right to restrict processing

a. Data subjects have a right to 'block' or suppress the processing of personal data. This means that the school can continue to hold the personal data but not do anything else with it.

b. The school must restrict the processing of personal data:
i) where it is in the process of considering a request for personal data to be rectified (see above).
ii) where the school is in the process of considering an objection to processing by a data subject.
iii) where the processing is unlawful, but the data subject has asked the school not to delete the personal data.
iv) where the school no longer needs the personal data but the data subject has asked the school not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the school.
v) If the school 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.

c. 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

a. 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.

b. An objection to processing does not have to be complied with where the 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.

c. In respect of direct marketing any objection to processing must be complied with.

d. The school 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. Our school does not currently take any decisions about individuals by automated means that have a legal affect in relation to an individual.

Annex D to
Data Protection Policy

APPROPRIATE POLICY DOCUMENT

1. **Scope.**

   a. 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.

   b. In order to operate effectively, the Federation has 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.

   c. The Federation 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**.

   a. Schedule 1, Part 1 – Conditions relating to employment, social security and social protection.
      i) Employment, social security and social protection.
      ii) Processing personal data concerning health in connection with our rights under employment law.
      iii) 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.

   b. Schedule 1, Part 2 – Substantial Public Interest Conditions
      i) **Statutory etc. and government purposes**
         1) Fulfilling the school's obligations under UK legislation for the provision of education to school aged children.
         2) Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.
         3) We may also process criminal offence data under this condition.
      ii) **Equality of opportunity or treatment**
         1) Ensuring compliance with the School's obligations under legislation such as the Equality Act 2010.
         2) Ensuring that we fulfil our public sector equality duty when carrying out our work.
         3) Ensuring we provide equal access to our services, to all pupils in recognition of our legal and ethical duty to represent and serve

pupils.

iii) **Preventing or detecting unlawful acts**
1) 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.
2) Disclosing data to support the prevention or detection of unlawful acts.

iv) **Protecting the public against dishonesty etc.**
1) Processing data concerning dishonesty, malpractice or other improper conduct in order to safeguard and protect pupils and the wider community.
2) Carrying out investigations and disciplinary actions relating to our employees.
3) Regulatory requirements relating to unlawful acts and dishonesty etc.
4) Assisting other agencies in connection with their regulatory requirements.

v) **Support for individuals with a particular disability or medical condition**
1) To provide services or raise awareness of a disability or medical condition in order to deliver services to individuals.

vi) **Counselling**
1) For the provision of confidential counselling organised through Occupational Health, advice or support or of another similar service provided confidentially.

vii) **Safeguarding of children and individuals at risk**
1) Protecting vulnerable children and young people from neglect, physical, mental or emotional harm.
2) Identifying individuals at risk while attending emergency incidents.
3) Obtaining further support for children and individuals at risk by sharing information with relevant agencies.

viii) **Insurance**
1) Information that is necessary for insurance purposes.

ix) **Occupational pensions**
1) Fulfilling the School's obligation to provide an occupational pension scheme.

c. Schedule 1, Part 3 – Additional Conditions Relating to Criminal Convictions, etc.
i) The Federation 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

a. Article 5 of the UK GDPR states that personal data shall be:
i) Processed lawfully, fairly and transparently.
ii) Collected for specific and legitimate purposes and processed in accordance with those purposes.

iii) Adequate, relevant and limited to what is necessary for the stated purposes.
iv) Accurate and, where necessary, kept up-to-date.
v) Retained for no longer than necessary, and
vi) Kept secure

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

c. **Processed lawfully, fairly and transparently**
i) The Federation provides clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices and policy documents.
ii) Our processing for purposes of substantial public interest are necessary to exercise our functions which are outlined in legislation.
iii) Our processing for the purposes of employment relates to our obligations as an employer.
iv) 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.
v) The Senior Leadership Team and Governors oversees policy work and monitors compliance in all areas of Information Governance, as outlined in its terms of reference.
vi) We carry out data protection impact assessments to ensure processing is fair and lawful.

d. **Collected for specific, explicit and legitimate purposes**
i) 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.
ii) We are authorised by law to process personal data for the purposes outlined above.
iii) We process personal data only when it is necessary and proportionate.
iv) If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.
v) 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.

e. **Adequate, relevant and limited to what is necessary for processing.**
i) We collect personal data necessary for the relevant purposes and ensure it is not excessive.

ii) 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.

f. **Accurate and kept up to date with every effort to erase or rectify without delay.**
   i) 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 Federation has processes in place to help people do this.
   ii) 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 don't apply, we will document our decision.

g. **Kept in a form such that the data subject can be identified only as long as is necessary for processing**.
   i) All data processed by the Federation, 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.
   ii) We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs.
   iii) Our retention schedule is reviewed regularly and updated when necessary.
   iv) We anonymise data when possible.

h. **Processed in a manner that ensures the appropriate security.**
   i) The Federation 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 School itself.
   ii) Both the School and its processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
   iii) When assessing appropriate organisational and technical measures, the School Business Manager (DPO) and Head Teacher will consult with other relevant services, such as ICT, Human Resources and Audit.
   iv) Our Senior Leadership Team and Governors meet regularly to ensure suitable information security governance is deployed throughout the Federation.
   v) Employees working within the Federation are to undertake a Disclosure and Barring Service (DBS) check.
   vi) All of our staff are trained in data protection matters and our contracts include confidentiality clauses.
   vii) Technical security controls such as encryption are employed to secure sensitive information within systems.
   viii) Role-based access controls are implemented to restrict access to sensitive data.

ix) Where possible, anonymisation or pseudonymisation are used to reduce the risk of sensitive data being compromised.

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

4. **Additional special category processing**. The Federation processes 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.

Annex E to
Data Protection Policy

ROLE OF THE DATA PROCESSING OFFICER

1. Purpose

a. 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 school's data protection processes and advise the school on best practice.

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

2. Data Protection Officer Responsibilities

a. To advise the school about their obligations under the General Data Protection Regulation 2016 and the Data Protection Act 2018.

b. To 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.

c. To assist, in cooperation with the DPL, with the monitoring of the school's compliance with data protection law, by:
   i) collecting information to identify data processing activities.
   ii) analysing and checking the compliance of data processing activities.
   iii) informing, advising and issuing recommendations to the school.
   iv) ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate.

d. To assist the DPL in making sure that the school's policies are followed, through:
   i) assigning responsibilities to individuals.
   ii) awareness-raising activities.
   iii) coordinating staff training.
   iv) conducting internal data protection audits.

e. To advise on and assist the school with carrying out data protection privacy impact assessments, if necessary;

   i) act as a contact point for the ICO, assisting and consulting it where necessary, including:
      a) helping the ICO to access documents and information.
      b) seeking advice on data protection issues.

f. To act as a contact point for individuals whose data is processed (for example, staff, students and parents), including:
   i) responding with support from the DPL to subject access requests.
   ii) responding with support from the DPL to other requests regarding individuals' rights over their data and how it is used.
   iii) take a risk-based approach to data protection, including:
      a) prioritising the higher-risk areas of data protection and focusing mostly on these.
      b) advising the school if / when it should conduct an audit, which areas staff need training in, and what the DPO / DPL roles should involve.

g. To report to the governing board on the school's data protection compliance and associated risks

h. To respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role.

i. To assist the DPL in maintaining a record of the school's data processing activities.

j. To work with external stakeholders, such as suppliers or members of the community, on data protection issues.

k. To work with the DPL in fostering a culture of data protection throughout the school.

l. To work closely with other departments and services to ensure UK GDPR compliance, such as HR, legal, IT and security.

m. To work with the Senior Leadership team at the school to ensure UK GDPR compliance.

n. To assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

3. Tasks

a. From these responsibilities, isolated tasks should include:

   i) providing a model Data Protection Policy and assist in customising it for the school.
   ii) advising on procedures and proformas to allow the Data Protection Policy to be adhered to.
   iii) providing advice on other associated policies and documents.
   iv) providing materials and advice in completing a dynamic Data Asset Audit and assisting in its completion if necessary.
   v) checking issues with the Data Asset Audit.

vi) providing training materials to allow the DPL to assist staff in keeping up to date with Data Protection issues.
vii) acting as the point of contact for SAR and FOI requests and supporting the school to provide the information as required.
viii) providing a Data Protection Audit on a 3 yearly rota basis and producing a report for Governors at cost.
ix) providing telephone and email advice and support.
x) providing regional training for the DPL and other staff.
xi) providing school based on-demand training at cost.

Annex F to
Data Protection Policy

ROLE OF THE DATA PROTECTION LEAD

1. Data Protection Lead Responsibilities

a. To verify that the school has registered with the ICO.

b. To support the DPO in advising the school about their obligations under the Data Protection Act 2018.

c. To support the DPO in developing an understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures.

d. To assist, in cooperation with the DPO, with the monitoring of the school's compliance with data protection law, by:
   i) collecting information to identify data processing activities.
   ii) analysing and checking the compliance of data processing activities.
   iii) informing, advising and issuing recommendations to the school.
   iv) ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate.

e. To assist the DPO in making sure that the school's policies are followed, through:
   i) assigning responsibilities to individuals.
   ii) awareness-raising activities.
   iii) coordinating staff training.
   iv) conducting internal data protection audits.

f. To act as a contact point for the DPO in supporting individuals whose data is processed (for example, staff, students and parents), including:
   i) responding with support from the DPO to subject access requests.
   ii) responding with support from the DPO to other requests regarding individuals' rights over their data and how it is used.

g. To assist the DPO in maintaining a record of the school's data processing activities providing this on a yearly basis to the DPO.

h. To assist the DPO in working with external stakeholders, such as suppliers or members of the community, on data protection issues.

i. To work with the DPO in fostering a culture of data protection throughout the school.

j. To work with the Senior Leadership team at the school to ensure UK GDPR compliance.

k. To assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

2. Tasks

a. From these responsibilities, isolated tasks should include:

i) acting as the point of contact with the DPO.
ii) assisting in customising the Data Protection Policy for the school.
iii) advising on procedures and proformas to allow the Data Protection Policy to be adhered to.
vi) providing advice on other associated policies and documents.
v) providing materials and advice in completing a Data Asset Audit and assisting in its completion if necessary.
vi) supplying the DPO with the Data Asset Audit on a yearly basis.
vii) using the training materials provided by the DPO to assist the staff in keeping up to date with Data Protection issues.

Annex G to
Data Protection Policy

DATA PROTECTION IMPACT STATEMENT

1. Before the use of any new service that uses personal data, staff should fill in a Privacy Impact Assessment Form.

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

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

4. The Federation will follow the guidance from the 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/

Privacy Impact Assessment Form

Privacy Impact Assessment (PIA) for:
Name of Service/Software/App

Data Protection Principles

a. Processing to be lawful and fair
b. purposes of processing be specified, explicit and legitimate
c. adequate, relevant and not excessive
d. accurate and kept up to date
e. kept for no longer than is necessary
f. processed in a secure manner

Why a Privacy Impact Assessment is required – screening questions

We need to complete this form because:

a. the use involves the collection of new information about individuals.
b. the use compels individuals to provide information about themselves.
c. the information about individuals will be disclosed to organisations or people who have not previously had routine access to the information.
d. we are using information about individuals for a purpose it is not currently used for, or in a way it is not currently used.
e. we are using new technology that might be perceived as being privacy intrusive, for example, the use of facial recognition.
f. the use results in us making decisions or acting against individuals in ways that can have a significant impact on them.

g. the information about individuals is of a kind particularly likely to raise privacy concerns or expectations, for example, health records, criminal records or other information that people would consider to be private.
h. the use requires us to contact individuals in ways that they may find intrusive.

Annex H to
Data Protection Policy

SUBJECT ACCESS REQUEST PROCESS

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

   a. inform the DPL in the school (and the Headteacher if necessary)

   b. record the details of the request, updating this record where necessary (see next page).

   c. reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required.

   d. contact the DPO if clarity on the request is needed or procedure is needed.

   e. identify the people responsible for gathering the necessary data.

   f. gather the data indicating a deadline.

   g. examine the data for redactions making sure there is no 'bleeding' of data.

   h. ask the requestor for an address and time for delivery.

2. The whole process should take no longer than **30 calendar days**, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

3. Please note the time for processing a request for an Educational Record in a maintained school is **15 days** (see section 9 in Data Protection Policy).

4. The Subject Access Requests are held on the P drive at each school (Admin / Office folders)

Subject Access Request Record

Name of data subject: _____

Name of person who made request: _____

Date request received: ____/____/____

Contact DPO (dposchools@somerset.gov.uk) : ____/____/____

Date acknowledgement sent: ____/____ /____

Name of person dealing with request: _____

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons and/or ask for proof
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, ask third parties to release external data. If data is supplied by another agency such as Psychology Service, you do not own the data.
Do you need to exempt/redact data?	If exempting/redacting be clear of your reasons Document name, data exempted/redacted, why.
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

At all stages, your DPO or DPL will be able to provide you with advice.

Date request completed: ____/____/____

(within 30 days of request)

Signed off by: _____

Describe the service			
Describe the data collected and the possible uses of the data			
List of data held	**Collection of data**		
	Possible uses		
Identify the privacy, related risks and possible solutions To be discussed with the Data Protection Lead			
Privacy issue	Risk to individuals	DPA Risks	Possible Solutions
1.	•	•	•
2.	•	•	•
3.	•	•	•
4.	•	•	•
5.	•	•	•
6.	•	•	•
Sign off and notes			
Comments on risks	Processes that must be in place		
Contact point for future privacy concerns Data Protection Officer: dposchools@somerset.gov.uk Data Protection Lead: A Person - aperson@educ.somerset.gov.uk Date completed: 24/01/2024			

Annex I to
Data Protection Policy

FREEDOM OF INFORMATION REQUEST PROCESS

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

   a. inform the DPL in the school (and the Headteacher if necessary).

   b. contact the DPO for clarity on the request and procedure, and a sample response.

   c. record the details of the request, updating this record where necessary (see next page).

   d. reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required.

   e. decide that if the material is already published or falls within an exemption.

   f. if data is not going to be published inform the requestor why this is not being released.

   g. identify the people responsible for gathering the necessary data.

   h. gather the data indicating a deadline.

   i. examine the data for redactions making sure there is no 'bleeding' of data.

   j. ask the requestor for an address and time for delivery.

2. 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.

3. The Freedom of Information requests are held on the P drive at each school (Admin / Office folders)

Freedom of Information Request Record

Name of person who made request: _____

Date request received: ____/____/____

Contact DPO (dposchools@somerset.gov.uk) : ____/____/____

Date acknowledgement sent: ____/____ /____

Name of person dealing with request: _____

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, then refer them to the correct agency
Do you need to exempt/redact data?	Could the data identify individuals Are any of the answers less than 5 people – use '5 or less including zero)? Are their commercial sensibilities?
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

At all stages, your DPO or DPL will be able to provide you with advice.

Date request completed: ____/____/____

(within 20 days of request)

Signed off by: _____

Annex J to
Data Protection Policy

DATA BREACH PROCESS

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

a. To inform the DPL in the school (and the Headteacher if necessary).

b. To record the details of the breach providing these details:
   i) a description of the nature of the personal data breach including, where possible.
   ii) the categories and approximate number of individuals concerned.
   iii) the categories and approximate number of personal data records concerned.
   iv) 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.
   v) a description of the likely consequences of the personal data breach.
   vi) 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.

c. To contact the DPO if clarity on reporting the breach is needed and if necessary, report to the ICO:

   i) by either by phoning 0303123 1113
   ii) by filling in the form at: https://cy.ico.org.uk/media/report-a-concern/forms/4019685/report-a-personal-data-breach-form.doc and sending it to icocasework@ico.org.uk
   iii) 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

d. To update the record where necessary (see next page).

e. To identify the people whose data is accidentally released, inform them of the breach and the processes taken to rectify the situation.

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

2. The Data Protection Breach records requests are held on the P drive at each school (Admin / Office folders)

Data Breach Record

Date: / /	Person responsible for dealing with breach				
Description of the nature of the personal data breach – how it occurred					
The categories and approximate number of individuals concerned					
The categories and approximate number of personal data records concerned					
A description of the likely consequences of the personal data breach					
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					
Reported by					
Phone/email sent to DPO dposchools@somerset.gov.uk	y/n	Is this high risk?	y/n	Report to ICO	y/n
Date reported to data subjects					
Notes					
Actions approved by		Date	/ /		

Annex K to
Data Protection Policy

CCTV POLICY

1. **Introduction**

a. At Merriott and Haselbury Plucknett Schools Federation, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our schools and its members.

b. The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the Federation and ensure that:
   i) We comply with the UK GDPR, effective 1 Jan 21.
   ii) The images that are captured are useable for the purposes we require them for.
   iii) We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation and their rights are being upheld.

c. This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:
Observing what an individual is doing.
Taking action to prevent a crime.
Using images of individuals that could affect their privacy.

2. **About this policy**.

a. This policy has been created with regard to the Home Office (2013) 'The Surveillance Camera Code of Practice' and Information Commissioner's Office (ICO) (2014) 'CCTV Code of Practice'.

b. This policy has due regard to legislation including, but not limited to, the following:
   i) The UK General Data Protection Regulation.
   ii) The Data Protection Act 2018.
   iii) The Freedom of Information Act 2000.
   iv) The Protection of Freedoms Act 2012.
   v) The Regulation of Investigatory Powers Act 2000

3. **Definition of data protection terms**. For the purpose of this policy a set of definitions will be outlined, in accordance with the Surveillance Camera Code of Practice:

a. **CCTV** – Closed Circuit Television is a system of cameras which stream an image to a central monitor, where activity can be recorded.

b. **Surveillance** – monitoring the movements and behaviour of individuals; through CCTV or BWC.

c. **Overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.

d. **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance. Merriott and Haselbury Schools Federation does not condone the use of covert surveillance when monitoring staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

4. **The Data Protection Principles and Privacy by Design**.

a. Data collected from surveillance and CCTV will be:
   i) Processed lawfully, fairly and in a transparent manner in relation to individuals.
   ii) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
   iii) Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
   iv) Accurate and, where necessary, kept up to date.
   v) Kept for no longer than is necessary for the purposes for which the personal data are processed.
   vi) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

b. The Federation will follow the ICO's guidelines on Privacy by Design – before planning installing and using a surveillance system, the Federation will:
   i) Consider whether the Federation can fulfil its requirements through a less privacy-intrusive system that does not include surveillance and recording.
   ii) Carry out a Data Privacy Impact Assessment (DPIA) to assess security risks and how the rights of individuals will be upheld.
   iii) Where the Federation identifies a high risk to an individual's interests, and it cannot be overcome, the Federation will consult the ICO before they use CCTV, and the Federation will act on the ICO's advice.

5. **Responsibilities of the Federation**

a. The Federation, as the corporate body, is the data controller. The governing board of Federation therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

b. The role of the data controller includes:
   i) Processing surveillance and CCTV footage legally and fairly.
   ii) Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.

iii) Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
iv) Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
v) Protecting footage containing personal data against accidental, unlawful destruction, alteration, and disclosure.

6. **Responsibilities of the Data Protection Officer**

a. As a Schools Federation we are data controllers in law and are required to appoint a Data Protection Officer. Our DPO is Amy Brittan and can be contacted at dposchools@somerset.gov.uk

b. The DPO is responsible for ensuring compliance with current Data Protection legislation and with this policy. Their responsibilities are laid out in the Data Protection policy, but in relation to CCTV and surveillance they include:
i) Ensuring that all data controllers at the Federation handle and process surveillance and CCTV footage in accordance with the 6 data protection principles.
ii) Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
iii) Supporting the Federation to complete a Data Privacy Impact Assessment when installing or replacing cameras.
iv) Reviewing the effectiveness of the current CCTV system and making recommendations if appropriate.
v) Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
vi) Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the Federation; their rights for the data to be destroyed and the measures implemented by the Federation to protect individuals' personal information.

7. **Responsibilities of the Headteacher**. The Headteacher has the following responsibilities:

a. Meeting with the DPO to decide where CCTV or BWC is needed to justify its means.

b. Liaising with the DPO regarding the lawful processing of the surveillance and CCTV footage.

c. Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.

d. Monitoring legislation to ensure the Federation is using surveillance fairly and lawfully.

e. Communicating any changes to legislation to all members of staff.

8. **Purpose and justification**

a. The Federation will only use surveillance cameras for the safety and security of the schools and its staff, pupils and visitors.

b. Surveillance will be used as a deterrent for violent behaviour and damage to the schools.

c. The Federation may share surveillance footage to assist the police in identifying persons who have committed an offence.

d. The Federation will only conduct surveillance as a deterrent and will not site cameras in classrooms or any changing facility.

e. The Federation may use surveillance data as part of disciplinary and grievance processes. This will be communicated to students and staff through the Federation Privacy Notices.

f. If the surveillance and CCTV systems fulfil their purpose and are no longer required the Federation will deactivate them.

9. **How the Federation manages CCTV and surveillance**.

a. The Federation is registered as a data controller with the Information Commissioner's Office, which also covers the use of surveillance systems.

b. CCTV warning signs are clearly and prominently placed at the Federation.

c. In areas where CCTV is used, the Federation ensure that there are prominent signs placed within the controlled CCTV area.

d. The surveillance system is a closed digital system will not record audio by default., as audio recording may be considered an excessive intrusion of privacy.

e. The surveillance system has been designed for maximum effectiveness and efficiency; however, the Federation cannot guarantee that every incident will be detected or covered and 'blindspots' may exist.

f. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

g. The surveillance system will not be trained on private vehicles or property outside the perimeter of the Federation.

10. Security

a. Access to the surveillance system, software and data is strictly limited to authorised school staff and is password protected.

b. The Federation 's authorised CCTV system users are the Executive Headteacher, the SLT, the Office Manager and the Office Administrator.

c. Visual display monitors are located in the main office at both schools and are password protected and locked at all times. The monitor screen is not in sight of the general public and is turned off when there is no requirement to view live images.

d. The main control facility is kept secure and locked when not in use.

e. Surveillance and CCTV systems will be checked for security flaws once a term to ensure that they are being properly maintained at all times.

f. The headteacher and authorised staff will decide when to record footage.

g. Any unnecessary footage captured will be securely deleted from the system.

h. Any cameras that present faults will be repaired immediately to avoid any risk of a data breach.

11. **Covert monitoring**.

a. The Federation may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.

ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

b. In these circumstances authorisation must be obtained from a member of the senior management team.

c. Covert monitoring must cease following completion of an investigation.

d. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

e. The Human Rights and Employment Rights of all the people who use the Federation must be respected and covert monitoring must only be used as a last

resort.

12. Storage and retention of images.

a. Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

b. The CCTV images will be kept for up to 40 days (in line with the purpose for recording this data) unless there is a current incident that is being investigated.

c. All retained data will be stored securely and will be listed on the Federation 's Data Asset Audit.

d. All retained data must be stored in a searchable system. Only a primary copy should be kept, and secondary copies should only be created in exceptional circumstances.

13. **Subject Access Requests (SARs)**

a. Individuals have the right to request access to video footage relating to themselves under the Data Protection Act 2018.

b. All requests should be made to the Headteacher or the Data Protection Officer. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example, date, time and location. Requests may be written or verbal.

c. The Federation will immediately indicate receipt and then respond within one calendar month of receiving the request.

d. The Federation reserves the right to refuse access to video footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

e. All attempts will be made to allow the viewing of the video. If others can be identified, the Federation will assess the risk to others from the video being viewed by the requester. If there is likely to be a risk of harm, the Federation may consider the following options where appropriate:
   i) Obtain the consent of others to share the video with the requester.
   ii) Use video-editing software to blur the faces of others who can be identified from the video.
   iii) Provide selected still images from the video and blur the identifiable faces.
   iv) Provide a transcript or written description of the contents of the video.

f. If all options have been considered and the Federation still consider there to be a risk to others from the requester viewing the video, the Federation may decline

the request to view the video (although relevant exemptions in the Data Protection Act 2018 will need to be identified by the Federation provided to the requester).

g. The Federation should not provide copies of the video to others unless instructed to do so in law or there is no risk to individuals who may be identifiable from the video.

14. **Access to and disclosure to other third parties**

a. There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the Federation where these would reasonably need access to the data (e.g. investigators) and with the correct authorisation.

b. Requests from third parties should be made in writing to the Headteacher or the Data Protection Officer. However, consideration must also be given to the following paragraph.

c. Consideration should always be given to the safeguarding and best interest of pupils. Data Protection should not be used as an excuse to prevent the viewing of images if there is an overwhelming need. All disclosures and the reasons for release should be recorded.

d. The data may be used within the Federation 's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures. This will be communicated to staff through the Federation Privacy Notices.

15. Complaints Complaints and enquiries about the operation of CCTV within the Federation should be directed to the Headteacher or the Data Protection Officer in the first instance.