Malmesbury C of E Primary School

Company Number 08483768

"Growing together in wisdom and love; discovering life in all its fullness."

Data Policy

Incorporating General Data Protection Regulation and Freedom of Information

Version: 1.1

Issue date:	May 2021
Reviewed date:	January 2024
Next Review:	January 2027

Malmesbury C of E Primary School
Tetbury Hill
Malmesbury
Wiltshire, SN16 9JR

Tel: 01666 823514

Headteacher: Stephen Heal

E-mail: admin@malmesbury-pri.wilts.sch.uk

1. Scope and Purpose of this Policy

1.1 This policy applies to all staff, governors (and volunteers where applicable) in the handling of data on behalf of and for Malmesbury C of E Primary School.

1.2 'Data' will include personal data (any information by which an individual might be identified) and financial (commercially sensitive) data.

1.3 This policy will be reviewed every two years by the Full Governing Body

1.3 Readers of this policy may also wish to refer to the school's e-Safety policy

2. Roles & Responsibilities

2.1 The school has a Data Protection Officer appointed by the Headteacher. He/she is responsible for:

- reviewing this policy for presentation to Governors;
- taking due regard for government requirements and guidelines regarding the use of data;
- policy implementation and monitoring including staff training;
- ensuring that any Freedom of Information and Subject Access Requests are responded to appropriately;
- together with the Headteacher, responding appropriately to any data breaches in the school to ensure that the impact of such is minimised whilst maintaining an open and honest manner in informing the appropriate stakeholders of the breach.

2.2 Other staff have particular responsibilities for data handling and controls as specified in their job descriptions.

2.3 It must be emphasised however that all staff must have due regard to data policies in carrying out their day-to-day work. All staff must ensure that data is processed within defined limits and for identifiable purposes, and that data is managed securely at all times.

3. The General Data Protection Regulation (GDPR) – replacing the Data Protection Act (1998)

3.1 The school complies with its duties under the GDPR (2018). The school is registered with the Information Commissioner's Office as a data controller.

3.2 Staff and governors should have due regard to the 6 principles of the Act. Data should be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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, using appropriate technical or organisational measures."

4. Data Processing Procedures

4.1 The school only holds the data which it deems to be necessary to: facilitate and enhance teaching and learning and pastoral care; ensure the safety of pupils and staff; and carry out appropriate administration.

4.2 An information audit map will be compiled and updated annually in Terms 5-6. This is known as the Information Asset Register (IAR).

4.3 A Data Protection Impact Assessment (DPIA) - sometimes referred to as a Privacy Impact Assessment (PIA) will be carried out as required but particularly when planning a new initiative that may involve 'high risk' data processing.

4.4 Privacy notices, as shown in the Staff and Pupil Privacy Notices (Appendices 1A and 1B), are issued annually to all staff and parents/carers of pupils to inform them that the school holds data on them and who the school may share this information with.

4.5 All data that is gathered, whether relating to pupils, staff or other stakeholders, is kept as up-to-date and accurate as possible. Data collection sheets are issued to parents/carers for checking on a rolling program if required or the information is collected electronically where possible. When the school is informed of a change to personal data, computer and papers records are updated as soon as practicable.

4.6 All staff and governors have a duty to ensure that data they hold is kept secure. Specific information regarding that can be found in the Acceptable Use Policy for Data (Appendix 2).

4.7 The school follows national guidelines regarding data retention. Paper copies of personal data will be shredded when no longer needed and electronic copies deleted. Hard drives are securely wiped when being disposed of. Educational records, including but not limited to SEN records, are stored until the pupil is 25, and then securely disposed of. Employee personnel records will be held for the length of

employment plus 7 years, before being securely disposed of, with the exception of documents relating to child protection or accidents at work which may be held for longer periods. A Retention of Records Table and Record Disposal Authorisation Form are provided in Appendices 3 & 4.

4.8 With regards to subject access requests, whereby any parent or member of staff may request access to their child's or their own personal data, the school complies with the GDPR and follows guidance from the Information Commissioner's Office. Access requests will be dealt with within one month of a written request being received.

4.9 Personal data belongs to the individual, even if the person is too young to understand the implications of subject access rights. In the case of young children these rights are likely to be exercised by those with parental responsibility for them, but all requests should be considered on that basis of the child is mature enough to understand their rights. If the Data Protection Officer (DPO) is confident that the child can understand their rights, then they should respond to the child rather than a parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, the DPO should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, the law presumes that a child aged 12 years or more has the capacity to make a subject access request. The presumption does not apply in England and Wales or in Northern Ireland, but it does indicate an approach that will be reasonable in many cases. It does not follow that, just because a child has capacity to make a subject access request, they also have capacity to consent to sharing their personal data with others – as they may still not fully understand the implications of doing so.

4.10 Data may be shared with the Local Authority, DfE and other schools to allow the school to fulfil its statutory obligations, or to enable the transfer of information when a pupil leaves or joins the school. Details of who we share data with and why are contained within the relevant Privacy Notice

5. The Freedom of Information Act

5.1 Malmesbury C of E Primary School is committed to the Freedom of Information Act (2000) and to the principles of accountability and general right of access to information, subject to legal exemptions.

5.2 Under the Act, any person has a legal right to ask for access to information held by the school. They are entitled to be told whether the school holds the information, and to receive a copy, subject to certain exemptions. Requests under the Freedom of Information Act are different to subject access requests (see section 4.8 above).

5.3 The school routinely makes information available to the public as defined in the Information Commissioner's Office model publication scheme. Much of this information can be found on the school website, or is otherwise available by contacting the school. Requests for other information will be dealt with in accordance with statutory guidance. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information.

5.4 Our process for responses to Freedom of Information requests is outlined in our Acceptable Use Policy for Data. (see Appendix 2). We have a duty to respond to all requests within 20 working days (excluding school holidays). Requests may be refused if:

- the estimated cost of complying exceeds £450
- the request is vexatious
- the request is for information previously supplied

5.5 Where information is subject to an absolute or qualified exemption under the Act, we will inform the person making the request of this, after invoking the public interest test procedures as appropriate. Any complaint made following this will be handled as per the school's complaints procedure.

5.6 The Data Protection Officer must be made aware of all Freedom of Information requests. A register of these will be kept.

6. Use of CCTV

6.1 Under the Protection of Freedoms Act 2012 the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the GDPR and the Information Commissioner's Office (ICO) has issued a code of practice on compliance with legal obligations under that set of regulations.

6.2 The school uses CCTV equipment to provide a safer, more secure environment for pupils and staff and for:

- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
- Safeguarding public, pupil and staff safety.
- Monitoring the security of the site.

The school does not use the CCTV system for covert monitoring.

6.3 Cameras are located in those areas where the school has identified a need and where other solutions are ineffective. The school's CCTV system is used solely for purposes(s) identified above.

6.4 The CCTV system is maintained by the school's Site Manager, who periodically inspect the cameras to ensure that date and time references are accurate, clear images are recorded and that as far as possible equipment is protected from vandalism.

6.5 In areas where CCTV is used the school ensures that there are prominent signs in places which are clearly visible and readable.

6.6 The school's standard CCTV cameras record visual images only and do not record sound. Where two way audio feeds (eg call for help systems) are used, they will only be capable of activation by the person requiring help.

6.7 The school has notified the Information Commissioner's Office of the purpose for which the images are used. All operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained in their responsibilities under the CCTV Code of Practice. Access to recorded images is restricted to staff that need to have access in order to achieve the purpose of using the equipment. All access to the medium on which the images are recorded is documented. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images. Under the Schools (Specification and Disposal of Articles) Regulations 2013, school staff can view CCTV footage in order to decide whether to search a pupil for an item. Footage may also be used for other disciplinary reasons.

6.8 Recorded images will be stored in a way that ensures the integrity of the image and in a way that allows specific times and dates to be identified. Access to live images is restricted to reception staff, the Site Manager and members of the Senior Leadership Team unless the monitor displays a scene which is in plain sight from the monitoring location.

6.9 Recorded images can only be viewed by approved staff. The recorded images are viewed only when there is suspected criminal activity, or activity which could be harmful to pupils and staff, and not for routine monitoring of pupils, staff or visitors.

6.10 The school reserves the right to use images captured on CCTV where there is activity that the school cannot be expected to ignore such as criminal activity, potential gross misconduct, or behaviour which puts others at risk. The retention of recordings for evidential purposes will be authorised by the Headteacher or a member of staff to whom this authorisation has been delegated to by the Headteacher.

6.11 The school ensures that images are not retained for longer than is necessary. CCTV systems are designed to overwrite the oldest recordings after a set period (currently 2 weeks).

6.12 Disclosure

Disclosure of the recorded images to third parties can only be authorised by the Headteacher or a member of staff to whom this authorisation has been delegated to by the Headteacher.
Disclosure will only be granted:

- If its release is fair to the individuals concerned.
- If there is an overriding legal obligation (eg information access rights).
- If it is consistent with the purpose for which the system was established.

All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented.
NB: Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

6.13 Subject access requests
Individuals whose images are recorded have a right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If the school receives a request, this will be handled as per section 4.8. As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and its disclosure is unlikely. Refusal to disclose images may also be appropriate where their release is likely to cause substantial and unwarranted damage to the individual, or to prevent automated decisions from being taken in relation to that individual.

7. Policy adoption

Signed Steve Heal (Headteacher): 

Date: January 2024

Signed Laurence Mussett (Chair of Governors): 

Date: January 2024

APPENDIX 1A – STAFF PRIVACY NOTICE

Privacy Notice – General Data Protection Regulation (2018) –
For the school workforce (those employed or otherwise engaged to work at a school)
We, Malmesbury C of E Primary School, are the Data Controller for the purposes of the GDPR.
Personal data is held by the school about those employed or otherwise engaged to work at the school. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Allowing better financial modelling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teachers' Review Body.

<u>The categories of school workforce information that we collect, process, hold and share include:</u>

- personal information required for payroll (such as name, address, employee or teacher number, national insurance number, bank details)
- special categories of data including characteristics information such as gender, age, ethnic group, relevant medical information and next of kin information.
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)

<u>Why we collect and use this information</u>
We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed.
- inform the development of recruitment and retention policies.
- enable individuals to be paid.
- permit better financial modelling and planning.
- enable ethnicity and disability monitoring.

<u>The lawful basis on which we process this information</u>
We process this information for general purposes under the requirements of the Education Act 1996 and the GDPR's following lawful bases:

1. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (Article 6, GDPR May 2018)

and for special category data; where

2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject. (Article 9, GDPR May 2018)

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information
We hold school workforce data for 7 years after an individual's employment has terminated.

Who we share this information with and why
We routinely share this information with:

- **Wiltshire Local Authority**
  We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

- **the Department for Education (DfE**)
  We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.
  We are required to share information about our pupils with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Data collection requirements
The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required

- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Tina Osborne, School Business Manager.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information
If you would like to discuss anything in this privacy notice, please contact Tina Osborne.

I have read and understood the regulations regarding the use of my personal data.

Name:_____

Signed:_____ Date:_____

APPENDIX 1B – PUPIL PRIVACY NOTICE

Privacy Notice – General Data Protection Regulation (2018) –
For all pupils at Malmesbury C of E Primary School

Malmesbury C of E Primary School is the data controller for the purposes of the General Data Protection Regulation Act. We collect personal information from you and may receive information about you from your previous school and the Local Authority. We hold this personal data to:

- Support your learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well we are doing.

The categories of pupil information that we collect, hold and share include:

- Personal identifiers (such as name, unique pupil number, address and contacts)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Admissions and attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical and dietary information
- Special educational needs and safeguarding information
- Behavioural information including exclusions
- School catering information
- Trips and activities

We store this data securely during your time at school and beyond for purposes of references, results checking etc.

Why we collect and use this information

We use the pupil data:

- to provide the child with an education
- to allocate appropriate teaching resources
- to facilitate transition to future schools or other settings
- to monitor and report on pupil progress
- to provide appropriate pastoral care and ensure pupil safety whilst in our care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We process this information for general purposes under the requirements of the Education Act 1996 and the GDPR's following lawful bases:

1. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (Article 6, GDPR May 2018)

and for special category data; where

1. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to members or to former members of the body or to persons

who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consents of the data subjects. (Article 9, GDPR May 2018)

Collecting Pupil Information
Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data
We hold pupil data for a maximum of 25 years from the pupil's date of birth.

Who we share pupil information with
We routinely share pupil information with:

- schools that the pupils attend after leaving us
- Wiltshire Local Authority
- the Department for Education (DfE)
- School Nursing Team (Virgincare)
- Other third parties with whom we engage for the purposes of educational activity.

Why we share pupil information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information about Individual Pupils) (England) Regulations 2013.

Data collection requirements:
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information about Individual Pupils) (England) Regulations 2013.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Admin Office.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact
If you would like to discuss anything in this privacy notice, please contact Melanie Warwick (School Business Manager).

I have read and understood the regulations regarding the use of my / my child's* personal data.

*(*Please delete as applicable)*

Signed: _____ Date: _____

If you are a parent signing on behalf of your child, please state the name of the child:_____

APPENDIX 2 – ACCEPTABLE USE POLICY FOR DATA

All staff, governors and volunteers should be aware of this agreement, and agree to follow it as a condition of their employment or involvement with the school. Failure to do so may result in disciplinary action.

It is vital that the school fulfil its obligations under the General Data Protection Regulation (2018) and Freedom of Information Act (2000). All staff are given training on this, however this Acceptable Use Policy has been put together to ensure that all staff are aware of and follow specific rules.

Data to which this AUP applies

1. Personal data is defined as data with two or more personal identifiers (e.g. name and address, name and date of birth).

2. Sensitive data is any data that could harm, discomfort or embarrass an individual if it were to become public or be made available to an unauthorised individual. For example SEN, racial or medical data, bank details, phone numbers.

3. This AUP also applies to other confidential data such as performance management documents.

Security of paper-based data

1. Staff are responsible for ensuring that data issued to them remains secure. On site this means keeping data away from being easily accessible by unauthorised personnel e.g. pupils. Staff should ensure photocopying is collected promptly when sent remotely to copiers.

2. If taking data off site, paperwork should be stored securely at all times. You should remain with the data when in transit, and store it in a secure area e.g. a locked cupboard.

3. Data should never be taken outside of the EU.

4. Particularly sensitive data, e.g. SEN or medical records, payroll details etc, should never be removed from the school site and must remain in a secure area e.g. locked cupboard, filing cabinet or office at all times.

5. All paper based records containing data should be securely shredded when no longer of use. You should not keep records beyond this time, unless advised otherwise (e.g. child protection records must be kept for longer).

Security of electronic data

1. Ensure that your passwords for access to the network, email, SIMS, Parentmail and all other data-sharing sites are strong passwords. You should change these on a regular basis, and not tell other members of staff or pupils your passwords.

2. Ensure that you lock or log out your computer when leaving it unattended, even for a short period of time. You are responsible for activity that takes places using your credentials, which can be monitored.

3. When storing data in shared areas of the school's IT network, ensure that this cannot be accessed by pupils. Name files appropriately.

4. Ensure that data is not visible to pupils or other unauthorised personnel. This includes any data in SIMS.net or Parentmail.

5. Data must not be stored on staff laptops or any electronic device outside of school without being encrypted and must comply with the GDPR. In general there should be no need to store data outside school.

6. If storing/transferring data using a removable device, this device must be an encrypted USB drive which will be supplied to you by the school on request. This USB drive should remain physically secure both in transit and when stored, in the same way as paper based records. It must not be taken out of the EU. Should this USB drive go missing, you must inform a Senior Leader immediately. When your employment with the school terminates, you should return the USB drive to the Site Manager for secure disposal. Data must not be copied from the encrypted USB drive onto any computer equipment used off school site (this includes home computers).

7. Photos and videos of pupils must only be taken using school owned devices. Any exception to this can only be authorised by the Headteacher. The placing of photos on websites and social media must be approved by the Headteacher or a member of staff to whom this approval has been delegated to by the Headteacher.

8. Files should be deleted from the network and encrypted USB drives when no longer needed, in line with the school's data retention policy. When deleting a file from a USB drive outside of school you should use shift and delete to avoid the risk of a copy of the file being stored in the recycle bin.

9. If you use your mobile device(s) to access school email you must make sure that they are protected with a password or pass-code logon. If your device is lost or stolen you must inform the Data Protection Officer or the Headteacher as soon as possible.

10. When you leave the school, be aware that your accounts for the network, email and other systems will be disabled when your contract ends. Any school-owned equipment provided to you in your role (eg: laptops, iPads etc) must also be returned to school when your contract ends.

Release of data to others

1. Staff may share information with each other regarding pupils as necessary in the performance of their duties, as long as this sharing of information is in the best interests of the pupils. The only exception to this is where a manager has explicitly stated that information is not to be shared.

2. When sharing data with another organization e.g. another school, you should check the legitimacy of the potential recipient. Wherever possible, school-to-school pupil data transfers will be made by the data admin staff using the secure Perspective Lite system. If you are unsure you should consult a member of the SLT or the Site Manager, and always check before sending data abroad.

3. Staff with access to data regarding other staff, such as contracts and pay scales, should ensure they have been granted permission to access this data by the Head or Deputy Head.
4. You should use your school provided email account for all email related to your work for the school. This system is managed by Oakford Technology, on behalf of the school. When emailing a non malmesbury-pri.wilts.sch.uk address, emails will pass outside of the school's security systems and therefore you should not send data to such an address without prior approval from a member of Senior Leadership.

5. The school takes any data breach very seriously. Should you become aware of any such breach, or the potential for one, you should inform a member of the SLT immediately.

Freedom of Information and Subject Access Requests

1. Any member of staff or the Governing Body may receive a subject access request for personal data, or a request for information under the Freedom of Information Act. Such requests will be made in writing or by email.

2. If you receive such a request, you should inform the Data Protection Officer immediately, or in his/her absence the Headteacher. The school has a legal duty to respond to requests within a time limit of 20 working days, so it is important that you pass on the request in a timely manner.

3. You should then await a response for the Data Protection Officer or Headteacher before sending a response to the request.

4. Staff should be aware that, in fulfilling requests, the school may be required to disclose the contents of emails. It is therefore vital that staff remain professional in all correspondence.

5. It is an offence to willfully conceal, damage or destroy information in order to avoid responding to an enquiry, so it is important that no records that are the subject of an enquiry are amended or destroyed

APPENDIX 3 – RETENTION PERIODS TABLE FOR ACADEMY STAFF RECORDS

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
ACCIDENTS AND HEALTH & SAFETY RECORDS HELD LOCALLY		
Accident books / Accident Records / reporting individual accidents	Adults – 6 years from date of last entry Children – DoB + 25 years	Legal

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
Records relating to staff accident/injury at work	Until 6 years after employment ceases	
Medical – Medical records for employees exposed to asbestos	40 years from the date of the last entry	Legal
Medical – Medical records for employees exposed to radiation	40 years from the date of the last entry	Legal
Medical – Medical Examination Certificates	4 years from the date of issue	Legal
COSHH Risk assessments & records	Current year + 10 years further	
H&S Risk Assessments	Until superseded but review every 12 month. If changed retain for current year + 6 years further	Legal
CONDUCT MATTERS – TRANSFERRED UNDER DUE DILIGENCE PRIOR TO TRANSFER AND HELD LOCALLY BY ACADEMY		
Letter of Suspension (as a neutral act)	Retain until investigation concludes whether a case to answer and follow guidance below on disciplinary records.	Policy
Disciplinary Action – no case to answer *(or if CP issue unsubstantiated/unfounded)*	Please see note above (in main body text) on child protection / safeguarding. If case does not relate to this destroy the record as soon as possible after the case is closed and within 6 months.	Policy
Disciplinary Action – Written Warning	12 months from date of warning	Policy
Disciplinary Action – Final Written Warning	18 months from date of final warning	Policy
Disciplinary Action – Dismissal	Unless relating to child protection allegations (see note above in	Policy

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
	main text body) 6 years after employment terminated	
Grievance / employee relations investigations	At least 3 years after procedural actions completed	Best Practice
EQUAL OPPORTUNITY RECORDS – HELD BY ACADEMY		
Equal Opportunities – Monitoring forms	Current year + 3 years in archive	Best Practice
Equal Opportunities – Policies	Current version + 1 year in archive after replacement	Best Practice
Equal Opportunities – Notice of requirement for an Action Plan	Recommended date of notice + 6 years	Legal
Equal Opportunities – Action Plan	Recommended date of Action Plan + 6 years	Legal
Equal Opportunities – Agreement	Recommended date of agreement + 6 years	Legal
Equal Opportunities – Compliance notice	Recommended date of compliance notice + 6 years	Legal
Equal Opportunities – Forms for use by a potential claimant / respondent	Recommended completion of action + 6 years	Legal
Disability forms for questions & replies	Throughout employment + 6 years after employment ceases	Legal
EMPLOYEE HANDBOOK – TRANSFERRED UNDER DUE DILIGENCE PRIOR TO TRANSFER AND HELD LOCALLY BY ACADEMY		
All HR Policies & Procedures adopted by the governing body	Hold as current documents made accessible for all staff on request until completely superseded by replacement policies. One copy of	Best Practice

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
	the old policy to be retained in Academy archive with the notes of the governing body's meeting which adopted the replacement policy.	
STAFF RECORDS TRANSFERRED UNDER DUE DILIGENCE PRIOR TO TRANSFER AND HELD LOCALLY BY ACADEMY		
HR Files generally all local HR records including training and working time records	6 years after employment ceases	Legal
Working Time – Record of Time Worked	2 years after the date which they were made	Legal
Teachers & Support Staff Personal Files	Current + 6 years archive after leaving	Best Practice
Teachers & Staff – Personnel Database (local)	Current information only	Legal
Supply Teacher's records	Current year + 2 years	Best Practice
Training records	Attach to staff personal file	N/A
Adoption Leave	Current year + 3 years archive	Best Practice
Notification for paternity leave for overseas adoption	3 years after application	Legal
Leave – Annual Leave	Current year + 1 year in archive	Best Practice
Leave – Jury Service	2 years after the period of jury service served	Best Practice
Leave – Special Leave	Current year + 1 year in archive	Best Practice
Leave – TOIL	Current year + 1 year in archive	Best Practice

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
Leave – Parental Leave	5 years from birth/adoption of the child or for 18 years if the child receives a disability allowance	Legal
Maternity – Leave, pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	Legal
Paternity – Leave, calculations, certificates	3 years after the end of the tax year in which the paternity period ends	Legal
Equal Pay Questionnaire & reply forms	Employment + 6 years after leaving	Legal
Probation reports and copy of probationary period outcome letter	Employment + 6 years after leaving	Legal
NQT records and report	At least 6 years after passing NQT induction year advised by DFe	Best Practice
Annual Appraisal/Performance Management Records	Current year and last 5 years	Best Practice
Redundancy – details of calculations of payments, notice (where paid rather than worked), collective and individual consultation notifications, letter of termination due to redundancy	6 years from the date of redundancy	Legal
Resignation letters	Hold on personal file in archive for 6 years after leaving date	Legal
Retirement	Hold on personal file in archive for 6 years after leaving date	Legal
Notification of death in service	Hold on personal file in archive for 6 years after death	Legal
Exit Questionnaire / notes of Exit Interview	Retain separate from personal file for 1 year after leaving date	Best Practice

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
TRADE UNION DOCUMENTS TRANSFERRED UNDER DUE DILIGENCE PRIOR TO TRANSFER AND HELD LOCALLY BY ACADEMY		
Recognition agreements, Collective agreements, Local agreements, Facility time agreements	10 years after ceasing to be effective	Legal
Joint Consultative Committee Agenda and Minutes (Held by LA)	Retain for master archives for future reference	Best Practice
Terms & Conditions Handbooks / NJC (Green Book & Burgundy Book)	Until completely superseded	Union / Best Practice
Notice of union learning representative	Whilst relevant + 3 years	Best Practice
JCC working papers (Held by LA)	Until they become policy + 3 years	Best Practice
RECRUITMENT RECORDS TO BE HELD BY THE ACADEMY		
Recruitment records of successful candidates including: • Formal Offer Letters • Record of DBS Clearance in Single Central Record (SCR) • Evidence of eligibility to work in the UK (copy) • Driving Licence (copy) • Medical Clearance (from OH) • Qualifications (copy)	For duration of the employment + 6 years after leaving	Legal
Adverts	Until post filled and copy of advert retained on personal file of successful candidate	Best Practice
Interview records/questions	Unsuccessful - date of interview + 6 months Successful - copy retained on personal file	Best Practice
Pre-DBS Disclosure risk assessment form	Until DBS Disclosure is received	Best Practice

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
Criminal records self-disclosure form	Until DBS Disclosure is received	Best Practice
References	Current Employment + 6 years in archive after leaving	
Application Form of Successful candidate	Current Employment + 6 years in archive after leaving	Best Practice
Recruitment Application forms	Unsuccessful – 6 months Successful - add to recruit's personal file	Best Practice
Job descriptions	Keep a copy of the current version & review annually	Best Practice
Job Evaluation documents	Keep a copy of the current version + 1 year in archive after leaving/changing	Best Practice
TRAINING RECORDS		
Attendance at training	Current year + 1 year archive	Best Practice
Training – Continuous Professional Development [CPD]	Add to personal file and destroy 6 years after employment ends	Best Practice
Training – Programme Materials	Whilst current	Best Practice
Training – Training records (other than youth records)	6 years after employment has ended	Best Practice
Post Entry Training	2 years after completion of qualification/course	Best Practice
TO BE KEPT BY THE ACADEMY'S HR & PAYROLL ADMINISTRATION PROVIDER		

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
Wage & Salary records (also overtime & bonus information)	Current year + last 6 years	Legal
Paternity Pay Entitlement	Current year + retain for 6 years	Legal
Statutory Sick Pay records, calculations, certificates, self certificates	Support staff - 3 years after the end of the tax year to which they relate. Teachers - 6 years after the end of the tax year to which they relate	Legal
Leave of Absence records	Current Year + 2 years archive	Best Practice
Honorarium records	Current Year + 2 years archive	Legal
TLR payment records	Current Year + 2 years archive	Legal
Golden Hello payments	Current Year + 2 years archive	Legal
Recruitment & retention payments	Current Year + 2 years archive	Legal
Overpayment recovery	Current Year + 2 years archive	Legal
Car mileage (P11D Detail)	Current Year + 6 years archive	Legal
Income tax P60	Current Year + 6 years archive	Legal/Best Practice
Maternity Payment	Current Year + 6 years archive	Best Practice
National Insurance – Schedule of payments	Current Year + 6 years archive	Legal
Overtime	Current Year + 2 years archive	Legal
Annual cost of living awards	Current Year + 6 years archive	Audit

NAME OF DOCUMENT	RETENTION PERIOD	REQUIREMENT
Payroll transactions	Current Year + 2 years archive	Legal
Payslip (copies)	Current Year + 6 years archive	Legal
Pension contributions record	Current Year + 6 years archive	Legal
Personal Bank Details	Until superseded + 2 years	Best Practice
Sickness records	Current year + 2 years archive	Best Practice
Staff returns for PD11	Current year + 2 years archive	Audit
Superannuation adjustments	Current year + 2 years archive	Legal
Superannuation reports (Annual)	Current year + 6 years archive	Legal
Tax forms (Inland Revenue)	Current Year + 6 years archive	Legal/Best Practice
Timesheets on working hours for claims for payment (casuals and variable hours staff)	Current Year + 2 years	Audit

Further detailed information

Further detailed information on document retention and disposal is available in the Information Records Management Society's (IRMS) School's Retention Schedule available at http://www.irms.org.uk/resources/848

APPENDIX 4 – RECORD DISPOSAL AUTHORISATION FORM

Academy name:							
I hereby certify that the records listed below have met the retention requirements of the Retention Schedule. Where appropriate, I have consulted with the information owner and any other relevant parties and can confirm I know of no reason why these records may not be disposed of in the manner indicated.							
Authorised by: (please print)		**Signature of Authoriser:**	**Position:**			**Date:**	
File Reference Number		**File Title**	**File Type**	**Format**		**Disposal action**	
				Paper	**Electronic**	**Archive**	**Destroy**

Disposed of by: **(please print)**		**Signature of Disposer:**	**Position:**			**Date of Disposal:**	