The Dharma Primary School

Data Protection Policy

1. Introduction

1.1. The Dharma Primary School regards the lawful and correct processing of personal and sensitive information/data as an integral part of its functions and vital for maintaining confidence between members, staff and other stakeholders whom we process information/data about and ourselves.

1.2. The Data Protection Act 1998 changed on 25 May 2018 with the implementation of the General Data Protection Regulation (GDPR). This is an EU Regulation that is directly effective in the UK and throughout the rest of Europe. A new Data Protection Act 2018 has also been passed to deal with certain issues left for national law: this includes specific provisions of relevance to independent schools. In particular, in the context of our safeguarding obligations, the School has a heightened duty to ensure that the personal data of pupils is at all times handled responsibly and securely.

While this new law does set out useful legal grounds in this area, in most ways this new law is strengthening the rights of individuals and placing tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and has powers to take action for breaches of the law.

2. Aims and Objectives

2.1 This Data Protection Policy explains how the Dharma Primary School will meet its legal obligations concerning confidentiality and information security standards. The requirements within the policy are primarily based upon the Data Protection Act 2018, which is the key piece of legislation covering information security and confidentiality of personal information. The objectives of this policy are to: -

- Establish a clear and agreed understanding of what confidentiality means within the Dharma Primary School
- Set out the way in which personal information/data should be protected and transferred within the Dharma Primary School
- Clearly state the Dharma Primary School's legal obligations to comply with Data Protection Act 2018
- Encourage uniformity in practice and ensure that staff, members and other stakeholders know what they can expect from the Dharma Primary School.

3. Definitions

3.1 **Personal information/data** relates to a living individual (a data subject), who can be identified from the information (or from that information and any other information in the possession of the Dharma Primary School. This includes name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that

it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.

3.2. **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

3.3. A **record** can be in computerised and/or manual form. It may include such documentation as:

- Hand written notes;
- Letters to and from the Dharma Primary School;
- Electronic records;
- Printouts;
- Photographs;
- Videos and tape recordings.

All data relating to an individual may need to be made available in response to a Subject Access Request (see section 7 below). Backup data also falls under the DPA; however, a search within them should only be conducted if specifically asked for by the data subject.

3.4. **Data Subject** – means an individual who is the subject of personal data.

3.5. **Data Controller** – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. For example, the School is the controller of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.

3.6 **Data Processor** – in relation to personal data, means any person who processes that data on behalf of the data controller other than an employee of the data controller, for example a payroll provider or other supplier of services.

3.7. **Third Party** - in relation to personal data, means any person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor.

3.8. **Processing** – means recording or holding information or data or carrying out any operations on that information or data; including organising, altering or adapting it; disclosing the information or aligning, combining, blocking or erasing it.

3.9. **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Policy Statement

4.1. The main focus of this policy is to provide guidance about the protection, sharing and disclosure of member/staff information, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to all staff and functions within the Dharma Primary School.

4.2. The Data Protection Act 2018 requires organisations to register with the Information Commissioner the categories of information they hold about people, and what they do with it.

4.3. The six Data Protection principles that lie at the heart of the DPA give the DPA its strength and purpose. To this end, the Dharma Primary School fully endorses and abides by the principles of data protection. Specifically, the six principles require that

1. Personal data must be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (accuracy).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (storage limitation)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (integrity and confidentiality).

The GDPR's 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data; and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

4.4. Personal data is defined in section 3 of this policy.

4.5. Compliance with these principles is the very essence of both compliance with the law and of good practice. The Information Commissioner's Office (ICO) has powers to interpret the principles and, subject to the interpretation provisions of the DPA, the Information Tribunal and the courts, to give advice about how to comply with the law, and enforce its provisions where this is necessary to achieve compliance. Understanding and complying with the principles is the key to understanding and complying with our responsibilities as a data controller.

4.6. Therefore, The Dharma Primary School will, through appropriate management, and strict application of criteria and controls:

- Ensure that there is a lawful ground for using the personal data and the use of the data is fair and transparent. (See Appendix I)
- Only use sensitive personal data if it is absolutely necessary for Dharma Primary School to use it. (See Section 3 – Paragraph 3.2)
- Only use sensitive personal data where the Dharma Primary School has obtained the individual's consent, which is freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- Explain to individuals, at the time their personal data is collected, how that information will be used.
- Only obtain and use personal data for those purposes which are known to the individual. If we need to use the data for other purposes, further consent may be needed.
- Only keep personal data that is really relevant and limited to Dharma Primary School.
- Where required keep personal data accurate and up to date.
- Only keep personal data for as long as is really necessary.
- Always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal data.
- Always allow individuals to opt-out of receiving marketing information. The DHARMA PRIMARY SCHOOL must always suppress the details of individuals who have opted out of receiving marketing information.
- Will always give an option to "opt out" when consent is needed to share personal data unless there is a statutory purpose to do so.
- Take appropriate technical and organisational security measures to safeguard personal data.

In addition, the Dharma Primary School will ensure that:

- There is a member of staff with specific responsibility for Data Protection (The Bursar is currently Data Privacy and Compliance Officer).
- Everyone managing and handling personal data understands that they are contractually (whether impliedly or expressly under their terms and conditions of employment) responsible for following good data protection practice.

- Everyone managing and handling personal data is appropriately trained to do so; and appropriate advice is available. Training and refresher training is a mandatory requirement for all staff every two years.
- Everyone managing and handling personal data is appropriately supervised.
- Enquiries about handling personal data are promptly and courteously dealt with.
- Methods of handling personal data are clearly described (See section 5 - Operational Practice).
- A regular review and audit is made of the way personal data is managed.
- Methods of handling personal data are regularly assessed and evaluated.
- Performance with handling personal data is regularly assessed and evaluated.

5. Operational Practice

5.1. Each staff member at Dharma Primary School should:

- Stop and consider whether they should be accessing or disclosing personal data before they do so.

- Make sure that they have verified that the person they are passing data on to is who they say they are and that they are authorised to receive it.

- Not discuss information about members, colleagues and other stakeholder with unauthorised colleagues, family or friends, or Dharma Primary School members.

- Not access Dharma Primary School business records containing personal data other than for a specific business purpose. This may also an offence under DPA and the member of staff may be prosecuted by ICO.

- Avoid providing any specific detail about individuals that might lead to their identification when using information for reports or monitoring purposes unless they have given written permission for it to be used.

- Not express unsubstantiated personal opinions in file notes or e-mails Individuals may have a right to see the information and may exercise that right.

- Give careful consideration to the use of e-mail distribution lists and use the blind carbon copy (BCC) option especially when sending out e-mails to large numbers of recipients (i.e. members or third parties).

- Always remember to consult their manager, and if necessary the Data Privacy and Compliance Officer for their input before starting any projects involving the processing of personal data.

- Always consider data security and the risks associated with losing personal data, before downloading/printing any personal data.

- Never share their computer password or write it down. Doing so could result in the unauthorised accessing of personal data and, therefore, a serious security breach.

- Always secure their screen when leaving their computer – even if it's only for a few minutes – and remember to log off at the end of the day.

- Never work on any Dharma Primary School data in a public place including use of mobile phones and laptops.

- Take care not to leave documents containing personal data on the printer, photocopier or scanner.

- Make sure that personal data cannot be seen or accessed by unauthorised individuals either in or out of the School and store it securely in a lockable cabinet. When travelling by car, papers must always be transported in the boot of the car. Papers must not be left in the car overnight; when at home they should be kept in a secured bag or cabinet.

- Remember to dispose of confidential waste and paper copies containing personal data in the **confidential waste bin** or by shredding.

- Ensure personal data extracted for Dharma Primary School use is stored on encrypted USB sticks or other suitable encrypted storage.

- Staff may extract data only with line management approval and the control of the data whilst extracted is the joint responsibility of the "data extractor" and their line manager.

- Understand what constitutes a data breach and report following correct procedure.

6. Transfer of Data to a Third Party

- Before personal data is transferred, a non disclosure agreement (NDA) should be in place between the Dharma Primary School and the third party. This agreement should clearly state the Third Party's obligation to treat the data in accordance with the provisions of the DPA the reasons for the transfer, the time period, what it is required for, how it will be processed and what actions will be taken to delete data when no longer needed.

- Non-disclosure agreements are managed by the Dharma Primary School Data Protection Officer and staff should ensure that they have checked with the Data Protection Officer that a NDA is in place before organising a transfer of personal data.

- Note that NDA is only valid for the data transfer within the EU and anything else is not permissible (unless special arrangements are made)

- Once an agreement is in place, data that is to be transferred through USB sticks or similar formats should be secured. Only encrypted USB sticks should be used. All data files should also be password protected. No such device should be sent through the open post – a secure courier service must always be used. The recipient should be clearly stated.

- If data is sent via a courier the intended recipient must be advised when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received, and liaising with the courier service if there is any delay in the receipt of the data.

7. Rights of Individuals and Data Access

Under the Data Protection Act 2018, any living person, who is the subject of personal data held and processed by the Dharma Primary School, has a right to apply for access to that information. This is known as a subject access request. (SAR) (See Appendix II)

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data

7.1. **What is a subject access request?**

- The Data Protection Act 2018 ensures transparency of processing personal data by obliging data controllers to explain to individuals how their data will be used, and by providing the right of data subjects to access that information.

- A data subject may make a formal request to any organisation to have a copy of all data in which that person may be identified. There is a need for transparency of processing to ensure that individuals can identify those organisations which have access to and process their data. This enables them to understand how their personal information is to be used and to exercise their rights over the processing of that information.

- The importance of the right of subject access in Data Protection law cannot be overestimated; it is often only by exercising the right to see their information that individuals can determine whether other breaches of legislation have occurred. Data

subjects are often interested in documentation, which may be about them, but they have not seen.

- Because of the importance of the subject access rights, complaints about an organisation's failure to comply with a request for subject access are taken very seriously by the Information Commissioner. Such complaints are dealt with as a matter of priority and may often lead to a full-scale investigation into an organisation's procedures and practices.

7.2. **What is a valid subject access request?**

- It must be in writing. A SAR can be made via email, fax, post or social media. Reasonable adjustments should be made if a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing.

- It must request access to their personal information (held either manually or electronically) and not to information relating to other people.

- If a request does not mention the Act specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.

- It may be restricted to only limited information (but need not be).

- It must be made by the data subject (or by a person authorised by the data subject). The Dharma Primary School will take reasonable steps to verify that the person making the subject access request is the data subject.

- It must be responded to the data subject within 72 hours to say that the request has been received and complied with within 30 calendar days from the date of receipt of the request

7.3. **Denial of Access**

The Dharma Primary School has the right to refuse a SAR on the following grounds:

- Repeat of earlier request access to personal information can be refused where an access request has previously been granted
- The material contains personal data of other people
- Requests from parties other than the subject
- Requests for access by other organisations
- Requests from the media

8. Roles and Responsibility

8.1. The Dharma Primary School has a duty to ensure that the requirements of the Data Protection Act 2018 are upheld.

8.2. The Dharma Primary School's Board of Trustees has overall responsibility for Data Protection within the Dharma Primary School. Trustees and Seniors Managers are responsible for information held manually and electronically within their functions and for development of procedures in relation to same. The responsibilities within parameters of this guidance include:

- The Trustees and Senior Management should be aware of their responsibilities to their staff and other individuals by becoming familiar with the Data Protection Policy.
- Informing the Data Privacy & Compliance Officer of any changes in the processing of personal data;
- Identifying and justifying how sets of data are used;
- Identifying all personal data for which they are responsible and;
- Agreeing who can have access to the data.

8.3. The Bursar has been appointed to the post of Data Privacy and Compliance Officer. Responsibilities of the Bursar and Head Teacher include:

- Ensuring compliance with legislation principles;
- Progressing any Data Protection Action Plan;
- Ensuring notification of processing of personal data to the information commissioner is up to date;
- Providing guidance and advice to staff in relation to compliance with legislative requirements;
- Reporting on any breaches of Data Protection legislation.

8.4. It is the responsibility of trustees, Bursar and Head teacher to ensure staff are aware of their obligations by producing relevant policy and providing training for existing staff.

- All staff handling personal information about members, staff, or individuals from other organisations are required to complete the online data protection training and read the policy, raising any questions and understanding them.
- Newly recruited staff are required to read Data Protection Policy provided via the "STAFF HANDBOOK" and to complete the online data protection training within the first month of joining the Dharma Primary School.

8.5. All Staff, Volunteers and Contractors are responsible for:

- Observing all guidance and codes of conduct in relation to obtaining, using and disclosing personal data;
- Obtaining and processing personal information only for specified purposes;
- Only accessing personal information that is specifically required to carry out their work;
- Recording information correctly in both manual and electronic records;
- Ensuring any personal information held is kept secure;
- Ensuring that personal data is not disclosed in any form to any unauthorised third party

- Ensuring sensitive personal information is sent securely. (See Section 9)
- Failure to adhere to any guidance in this policy could result in staff individually being criminally liable for deliberate unlawful disclosure under the Data Protection Act 2018. This may result in criminal prosecution and/or disciplinary action.

8.6. The Information Commissioner's Office is responsible for overseeing compliance (e.g. investigating complaints, issuing codes of practice and guidance, maintaining a register of data protection officers). Any failure to comply with the
DPA may lead to investigation by the ICO which could result in serious financial or other consequences for the Dharma Primary School and/or its members.

9. Sending Personal Sensitive information externally

Confidentiality

All staff have a duty to ensure that information about pupils, parents, staff and sensitive non-personal information is handled appropriately. Sensitive information should only be made available to people authorised to view it.

The following principles should be followed wherever you communicate sensitive personal information:

- Justify the purpose for sharing the information

- Do not use information that personally identifies individuals unless necessary.

- Information should be disclosed on a "need to know" basis.

- If unsure then seek guidance on appropriate action from the Data Privacy and Compliance Officer

Face to face

Personal information should not be shared in front of others. Staff should ensure that they are not disclosing or requesting the disclosure of sensitive information about themselves in front of others, e.g. in reception areas or in a format, that could be viewed by others.

Telephone

Personal information should only be disclosed over the telephone to a third-party where the following procedure has been adhered to:

- The identity of the other party has been confirmed by verification. The type of verification will differ by service and the sensitivity of the information being disclosed.

- The reason for requesting the information has been established and is appropriate.

- Where appropriate, contact details have been requested and their identity checked by calling the person back via the main switchboard of the organisation that they represent and asking for the person by name.

- Provide personal information only to the person who requested it.

- Do not leave any confidential information on voicemail or answering machines as it may be accessible by others. Please remember that by confirming an individual is a member of the Dharma Primary School you are releasing sensitive personal information as defined by the Data Protection Act.

- When in conversation take precautions to ensure that information is not shared inappropriately with others, e.g. when using mobile phones, travelling on trains, etc.

- Sensitive personal information should not be sent via text messaging as it may be accessible by others.

Email

Email services should be used as follows:

- Sensitive information relating to a single individual can be sent via email to the subject of the information if they have requested it to be sent by email or with their agreement and it is encrypted. The exception for this is when a member of the school has stated that they want to receive the information without encryption. A record must be kept of this. Documents containing sensitive personal information cannot be sent to third parties without encryption.

- Care should be taken when addressing email messages to ensure a correct, current address is used and the email is only copied to those with a legitimate interest.

- If information is transmitted and not received by the intended recipient, check that contact details and email address are correct for the receiving party before re-sending.

- Consider the impact on individuals of the data being lost or misdirected. Where information is provided in bulk or where the information is of a sensitive nature make an assessment on the protection to be applied. If in doubt, send information in an encrypted attachment to the email.

- Avoid putting sensitive personal information about more than one person in an email as this will lead to difficulties in maintaining accurate and relevant individuals or staff records.

- When transferring data be aware of who has permission to view your emails or who might be able to view your recipient's inbox.

10. Disposal of records/retention of data

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

- Paper records should be shredded or disposed of using a confidential waste bin
- CDs / DVDs should be cut into pieces
- Audio / Video Tapes should be dismantled and shredded
- All electronic forms of data storage will be disposed of via a reputable disposal company

Pupil data retention

Data type	Retention period
All records relating to the creation and implementation of the School Admissions' Policy	Life of the policy + 3 years then review
Admissions – if the admission is successful	Date of admission + 1 year
Admissions – if the appeal is unsuccessful	Resolution of case + 1 year
Admission Registers	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.
Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	DOB of the pupil + 25 years
Child Protection information held on pupil file	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.
Child protection information held in separate files	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record
Special Educational Needs files, reviews and Individual Education Plans	DOB of the pupil + 25 years
Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]
Advice and information provided to parents regarding educational needs	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]
Accessibility Strategy	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]

Attendance Registers	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.
Correspondence relating to authorized absence	Current academic year + 2 years
Examination results – Internal examination results	Current year + 5 years
SATS records –	The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison
Any other records created in the course of contact with pupils	Current year + 3 years then review
Schemes of Work	Current year + 1 year
Timetable	Current year + 1 year
Class Record Books	Current year + 1 year
Mark Books	Current year + 1 year
Record of homework set	Current year + 1 year
Pupils' Work	Where possible pupils' work should be returned to the pupil at the end of the academic year or securely disposed of
Parental consent forms for school trips where there has been no major incident	Conclusion of the trip
Parental permission slips for school trips – where there has been a major incident	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils
Images used in identity systems	Pupil at school + 1 month
Images used in educational displays and/or as a teaching aid	Pupil at school + 1 month
images used in general displays in school	Pupil at school + 1 year if active informed consent has been given at the time the photograph was taken
Images used in marketing (website/prospectus/video)	Pupil at school + 1 year if active informed consent has been given at the time the photograph was taken
Biometrics	Biometric data (typically fingerprints used in things like catering) should be used and retained as set out in the active informed consent gained at the outset, but typically this should not be retained long after the activity that requested its use has finished (for example, the child no longer attends the school to have a meal).

Head Teacher and Senior Management Team

Data type	Retention period
Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	Date of the meeting + 3 years then review
Reports created by the Head Teacher, the Senior Management Team and other members of staff with administrative responsibilities	Current academic year + 6 years then review
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Date of correspondence + 3 years then review
Professional Development Plans	Life of the plan + 6 years
School Development Plans	Life of the plan + 3 years
Records relating to the creation and publication of the school brochure or prospectus	Current year + 6 years
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current year + 1 year
Newsletters and other items with a short operational use	Current year + 1 year
Visitors' Books and Signing in Sheets	Current year + 6 years then REVIEW
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	Current year + 6 years then REVIEW
Attendance Returns	Current year + 1 year
School Census Returns	Current year + 5 years
Circulars and other information sent from the Local Authority	Operational use
ISI/ OFSTED reports and papers	Life of the report then REVIEW
Returns made to central government	Current year + 6 years
Circulars and other information sent from central government	Operational use

Human resources

Data type	Retention period
All records leading up to the appointment of a new Head Teacher	Date of appointment + 6 years
All records leading up to the appointment of a new member of staff – unsuccessful candidates	Date of appointment of successful candidate + 6 months
All records leading up to the appointment of a new member of staff – successful candidate	All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months
Pre-employment vetting information – DBS Checks	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months
Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file
Pre-employment vetting information – Evidence proving the right to work in the United Kingdom	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years
Staff Personal File	Termination of Employment + 6 years
Annual appraisal/ assessment records	Current year + 5 years
Timesheets	Current year + 6 years

Trustees

Data type	Retention period
Agendas for Trustee meetings	One copy should be retained with the master set of minutes. All other copies can be disposed of.
Minutes of Trustee meetings	One copy must be kept permanently as a master set. There may be data protection issues if the meeting is dealing with confidential issues relating to staff. If these minutes contain any sensitive, personal information, they must be shredded.
Action plans created and administered by the Trustees	Life of the action plan + 3 years
Internal inspection copies	These are the copies which the clerk to the governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made. Date of meeting + 3 years If these minutes contain any sensitive, personal information, they must be shredded.
Reports presented to the Trustees	Reports should be kept for a minimum of 6 years. However, if the master set of minutes refer directly to individual reports then the report should be kept permanently.
Policy documents created and administered by the Trustees	Life of the policy + 3 years
Records relating to complaints dealt with by the Trustees	Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes

Financial Management of the School

Data type	Retention period
Inventories of furniture and equipment	Current year + 6 years
Burglary, theft and vandalism report forms	Current year + 6 years
Annual Accounts	Current year + 6 years
Loans and grants managed by the school	Date of last payment on the loan + 12 years then REVIEW
All records relating to the creation and management of budgets including the Annual Budget statement and background papers	Life of the budget + 3 years
Invoices, receipts, order books and requisitions, delivery notices	Current financial year + 6 years
Records relating to the collection and banking of monies	Current financial year + 6 years
Records relating to the identification and collection of debt	Current financial year + 6 years

All records relating to the management of contracts under seal/ signature	Last payment on the contract + 12 years
Records relating to the monitoring of contracts	Current year + 2 years

Health and Safety

Data type	Retention period
Health and Safety Policy Statements	Life of policy + 3 years
Health and Safety Risk Assessments	Life of risk assessment + 3 years
Records relating to accident/ injury at work	Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied
Accident Reporting - Adult	Date of the incident + 6 years
Accident Reporting - Children	DOB of the child + 25 years
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	Last action + 40 years
Fire Precautions log books	Current year + 6 years
Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	Last action + 50 years
Control of Substances Hazardous to Health (COSHH)	Current year + 40 years

Management of Disciplinary and Grievance Processes

Data type	Retention period
Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned
Disciplinary Proceedings	
Oral warning	Date of warning + 6 months
Written warning – level 1	Date of warning + 6 months
Written warning – level 2	Date of warning + 12 months
Final warning	Date of warning + 18 months
Case not found	If the incident is child protection related then see above otherwise dispose of at the conclusion of the case

11. Breach of Policy

In the event that an employee fails to comply with this policy, the matter may be considered as misconduct and dealt with in accordance with the Dharma Primary School's Disciplinary Policy and procedure.

11.1. **Dealing with a Data Breach**
A data breach is a breach of security, which leads to any of the following:

- the loss of Personal Data;
- the accidental or unlawful destruction of Personal Data;
- the disclosure of Personal Data to an unauthorised third party;
- the unlawful or accidental alteration of Personal Data; or
- unauthorised access to Personal Data.

If staff are in any doubt as to whether an incident constitutes a data breach they must speak to the Bursar and immediately

- Notify the Chair of Trustees/ Head teacher
- Notify the Data Privacy and Compliance Officer

Following notification the Dharma Primary School will take the following actions urgently:-

- Implement a recovery plan, including damage limitation;
- Assess the risks associated with the breach;
- Inform the appropriate people and organisations that the breach has occurred;
- Review our response and update our information security;
- Notify the ICO within 72 hours.

Person Responsible for reviewing this policy	CM/Bursar
Date of last review	12/15
Date of this review	08/18
Date of next review	08/20

Appendix I

The Lawful bases for Processing

This section explains the lawful bases for processing that need to be satisfied before you may process personal data.

In brief – what does the Data Protection Act say about the "conditions for processing"?

The first data protection principle requires, among other things, that the Dharma Primary School must be able to satisfy one or more "conditions for processing" in relation to its processing of personal data. Many (but not all) of these conditions relate to the purpose or purposes for which it intends to use the information.
The conditions for processing take account of the nature of the personal data in question. The conditions that need to be met are more exacting when the information being processed is sensitive personal data, such as information about an individual's health or criminal record or trade union membership.
However, the ICO view is that in determining if there is a legitimate purpose for processing personal data, the best approach is to focus on whether what the organisation intends to do is fair. If it is, then it is likely to be possible to identify a condition for processing that fits that purpose.

Being able to satisfy a condition for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must still be looked at separately. So it makes sense to ensure that what the organisation wants to do with personal data is fair and lawful before worrying about the conditions for processing set out in the Act.

In more detail…What are the conditions for processing?

The conditions for processing are set out in Schedule 9 and Part 4 to the Data Protection Act 2018. Processing shall be lawful only if and to the extent that at least one of the following six legal bases applies:
(a) Consent (under GDPR, the definition of what constitutes consent has been tightened (and the fact that it can be withdrawn by the data subject) the Dharma Primary School should rely on another lawful ground where possible. the Dharma Primary School ensure the consent is clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable.)
(b) Contract: the processing is necessary for a contract with the individual
(c) Legal obligation: the processing is necessary to comply with the law
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary to perform a task in the public interest or for the official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, where the data subject is a child.

What is the "legitimate interests" condition?

The Data Protection Act recognises that organisations may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided certain requirements are met.

The first requirement is that the DHARMA PRIMARY SCHOOL must need to process the information for the purposes of its legitimate interests or for those of a third party to whom it discloses it.

The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. The Dharma Primary School's legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

What conditions need to be met in respect of special category data?

At least one of the conditions must be met whenever personal data is processed. However, if the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) 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;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) 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 the 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 consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

In addition to the above conditions – which are all set out in the Data Protection Act itself – regulations set out several other conditions for processing sensitive personal data. Their effect is to permit the processing of sensitive personal data for a range of other purposes – typically those that are in the substantial public interest, and which must necessarily be carried out without the explicit consent of the individual. Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration. A full list of the additional conditions for processing is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.

When is processing "necessary"?

Many of the conditions for processing depend on the processing being "necessary" for the particular purpose to which the condition relates. This imposes a strict requirement, because the condition will not be met if the organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way.

What is meant by "consent"?

One of the conditions for processing is that the individual has consented to their personal data being collected and used in the manner and for the purposes in question.

The circumstances of each case will need to be examined to decide whether consent has been given. In some cases this will be obvious, but in others the particular circumstances will need to be examined closely to decide whether they amount to an adequate consent.

Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual's consent as:

"…any *freely given* specific and informed indication of his wishes by which the data subject *signifies his agreement* to personal data relating to him being processed".

The fact that an individual must "signify" their agreement means that there must be some active communication between the parties. An individual may "signify" agreement other than in writing, but consent should not be inferred if an individual does not respond to a communication – for example, from a failure to return a form or respond to a leaflet.

Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. For example, if the DHARMA PRIMARY SCHOOL intends to continue to hold or use personal data after the relationship with the individual ends, then the initial consent to the processing of personal data should cover this.

Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in the information is collected or used. Withdrawing consent does not affect the validity of anything already done on the understanding that consent have been given.

Whether consent has been given is an issue that should be reviewed as the relationship with an individual develops, or as the individual's circumstances change.
Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

The Data Protection Act distinguishes between:

- The nature of the consent required to satisfy the first condition for processing; and
- The nature of the consent required to satisfy the condition for processing sensitive personal data, which must be "explicit".

This suggests that the individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the

purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

For these reasons the Dharma Primary School should not rely exclusively on consent to legitimise its processing. In the Information Commissioner's Office view it is better to concentrate on making sure individuals are treated fairly rather than on obtaining consent in isolation. Consent is the first in the list of conditions for processing set out in the Act, but each condition provides an equally valid basis for processing personal data.

For further information you can contact the ICO hotline which gives advice to the public and organisations on data protection/confidentiality or visit the link below:-

http://www.ico.gov.uk/

Appendix II

Data Access Request Form

Please note that whilst it is not obligatory to complete this form but information contained within it would help the Dharma Primary School to respond to your request in the most efficient manner.
Name:
Address:
Position if staff member:
Telephone Number:
By completing this form you are making a request under the Data Protection Act 2018 for information held about you by Dharma Primary School that you are eligible to receive.
Required information:
By signing below you indicate that you are the data subject named above. The Dharma School cannot accept requests from anyone else such as family members regarding your personal data. We may need to contact you for further identifying information before dealing with your request. You warrant that you are the data subject and will fully indemnify us for all losses, cost and expenses if you are not. Please return this form to the school Bursar via email (cmoody@dharmaschool.co.uk) or by post at The Dharma Primary School, 149 Ladies Mile Road, Brighton, BN1 8TB. Please allow 30 days for a reply.
Data subject's signature and date ……. ……..