GDPR – Compliant Records Management Policy

Author	Written / Reviewed	Passed by Governors	Next Review
K Appleby	June 2018	July 2018	June 2020

Contents

Statement of Intent

Shenstone Lodge School is committed to maintaining the confidentiality of its information and ensuring that all records within the School are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), the School also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The School has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet its statutory requirements. This policy applies to all records created, received, maintained or processed by staff of the School in undertaking its functions. Records are defined as all documents which facilitate the business carried out by the School and are retained for a period of time which has been defined, in order to provide evidence of its transactions and activities. Documentation may be processed as hard copies or in electronic format.

This document complies with the requirements set out in the GDPR, which will come into effect on 25th May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The retention periods outlined in this policy are good practice guidelines only, and the School should ensure that they consider requirements specific to their setting when implementing these timeframes. Where guidance for disposal methods or retention periods has not been provided, good practice recommendations have been provided in **yellow and bold**.

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:
- General Data Protection Regulation (2016)
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

1.2. This policy also has due regard to the following guidance:
- Information Records Management Society 'Information Management Toolkit for Schools' 2016

1.3. This policy will be implemented in accordance with the following School policies and procedures:
- Data Protection Policy
- Freedom of Information Policy
- E-security Policy
- Security Breach Management Plan

2. Responsibilities

2.1. The School as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2. The Executive Headteacher holds overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The Data Protection Officer supports the management of records.

2.4. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis,

2.5. The Admin Support Team is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.

2.6. All staff members are responsible for ensuring that any records for which they are responsible are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

2.7. The DPO is responsible for ensuring that any contracts held with third parties who process personal identifiable information (considered as data processors as outlined in the GDPR) are compliant with the GDPR.

2.8. Pupils and their parents (dependant on the age of the pupil and the age of consent according to UK derogation) have a right of access to their educational record under the GDPR and Educational (Pupil Information England) Regulations 2005. Shenstone Lodge School promotes the accurate and professional recording of all information.

3. Management of pupil records

3.1. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and include all personal information relating to them, e.g. date of birth, home address, medical information, as well as their progress, achievement and behaviour records.

3.2. The following information is stored in a pupil record and will be accessible to the appropriate personnel in accordance with their delegation of duties:

- Forename, surname, gender and date of birth
- Unique pupil number
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate
- Ethnic origin, religion and first language (if not English)
- Any preferred names
- Gender
- Position in their family, e.g. eldest sibling
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of parents, including their home address(es) and telephone number(s)
- Name of the School, admission number, the date of admission and the date of leaving, where appropriate
- Any other agency involvement, e.g. speech and language therapist
- Admissions form
- Details of any SEND
- Attendance to an early years setting, the record of transfer
- Annual written reports to parents
- Any reports written about a child
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the pupil
- Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan
- Any notes indicating child protection disclosures and reports are held
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Notes indicating that records of complaints made by parents or the pupil are held
- Privacy notices
- Absence notes
- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Correspondence with parents about minor issues, e.g. behaviour

3.3. Hard copies of disclosures and reports relating to child protection are stored in a locked cabinet in the Safeguarding Manager's Office.

3.4. Hard copies of complaints made by parents or pupils are stored in the pupil's record.

3.5. Actual copies of accident and incident information are stored separately on the School's management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

3.6. The School will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.

3.7. The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, the Admin Officer responsible for disposing records, will remove these records and appropriately dispose of them.

3.8. Electronic records relating to a pupil's record will also be transferred to the pupils' next school. Section 10 of this policy outlines how electronic records will be transferred.

3.9. The School will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post

4. Retention of pupil records and other pupil-related information

4.1. The table below outlines the retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.

4.2. Electronic copies of any information and files will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Admissions		
Register of admissions	Three years after the date on which the entry was made	Information is reviewed and the register may be kept permanently
Secondary school admissions	The current academic year, plus one year	Securely disposed of
Proof of address (supplied as part of the admissions process)	The current academic year, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Added to the pupil's record	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Until the appeals process has been completed	Securely disposed of
Pupils' educational records		
Primary Pupils' educational records	Whilst the pupil remains at the school	Transferred to the next destination – if this is an independent school, home-schooling or outside of the UK, the file will be kept by the LA and retained for the statutory period
Secondary Pupils' educational records	25 years after the pupil's date of birth	Securely disposed of

Public examination results	Added to the pupil's record	Returned to the examination board
Internal examination results	Added to the pupil's record	Securely disposed of
Child protection information held on a pupil's record	Stored in a sealed envelope for the same length of time as the pupil's record	Securely disposed of – shredded
Child protection records held in a separate file	25 years after the pupil's date of birth	Securely disposed of – shredded
Attendance		
Attendance registers	Last date of entry on to the register, plus three years	Securely disposed of
Letters authorising absence	Current academic year, plus two years	Securely disposed of
SEND		
SEND files, reviews and individual education plans	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the school to defend themselves in a 'failure to provide sufficient education' case
Statement of SEN maintained under section 324 of the Education Act 1996 or an EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Curriculum management		
SATs results	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of

Examination papers	Until the appeals/validation process has been completed	Securely disposed of
Published Admission Number (PAN) reports	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms	Current academic year, plus six years	Securely disposed of
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of
Extra-curricular activities		
Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip	Securely disposed of
Parental consent forms for school trips where a major incident occurred	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Securely disposed of
Walking bus registers	Three years from the date of the register being taken	Securely disposed of
Day books	Current academic year, plus two years	Reviewed and destroyed if no longer required
Reports for outside agencies	Duration of the pupil's time at school	Securely disposed of
Referral forms	Whilst the referral is current	Securely disposed of
Contact data sheets	Current academic year	Reviewed and destroyed if no longer active
Contact database entries	Current academic year	Reviewed and destroyed if no longer required
Group registers	Current academic year, plus two years	Securely disposed of

5. Retention of staff records

5.1. The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.
5.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personal file	Termination of employment, plus six years	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of
Recruitment		
Records relating to the appointment of a new Principal	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
DBS certificates	The School does not keep copies of DBS certificates but must be able to evidence in writing that they have been checked.	Securely disposed of if copies taken
Proof of identify as part of the enhanced DBS check	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, securely disposed of
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of

Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personal files	Reviewed and securely disposed of – shredded
Oral warnings	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 1	Date of warning, plus 6 months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 2	Date of warning, plus 12 months	Securely disposed of – if placed on staff personal file, removed from file
Final warning	Date of warning, plus 18 months	Securely disposed of – if placed on staff personal file, removed from file
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of as above	Securely disposed of

6. Retention of senior leadership and management records

6.1. The table below outlines the School's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Governing board		
Agendas for Governing Body meetings	One copy alongside the original set of minutes – all others disposed of without retention	Securely disposed of
Original, signed copies of the minutes of Governing Body meetings	Permanent	Archived in cellar
Inspection copies of the minutes of governing board meetings	Date of meeting, plus three years	Shredded if they contain any sensitive and personal information
Reports presented to the Governing Board	Minimum of six years, unless they refer to individual reports – these are kept permanently	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes
Instruments of government, including Articles of Association	Permanent	
Action plans created and administered by the Governing Board	Duration of the action plan, plus three years	Securely disposed of
Policy documents created and administered by the Governing Board	Duration of the policy, plus three years	Securely disposed of
Records relating to complaints dealt with by the Governing Board	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus 10 years	Securely disposed of
Proposals concerning changing the status of the School	Date proposal accepted or declined, plus three years	Securely disposed of

Senior leadership team (SLT)		
Log books of activity in the School maintained by the Exec Head	Date of last entry, plus a minimum of six years	Reviewed and offered to the School archives if appropriate
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed and securely disposed of
Reports created by the Exec Head or SLT	Date of the report, plus a minimum of three years	Reviewed and securely disposed of
Records created by the Exec Head and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed and securely disposed of
Correspondence created by the Exec Head and members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed and securely disposed of
Professional development plan	Duration of the plan, plus six years	Securely disposed of
School Development Plan	Duration of the plan, plus three years	Securely disposed of

7. Retention of health and safety records

7.1. The table below outlines the School's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.

7.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and safety		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of

Accident reporting – adults	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	25 years after the pupil's date of birth, on the pupil's record	Securely disposed of
Control of substances hazardous to health	Current academic year, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Securely disposed of
Fire precautions log books	Current academic year, plus six years	Securely disposed of

8. Retention of financial records

8.1. The table below outlines the School's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

8.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll pensions		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
Risk management and insurance		
Employer's liability insurance certificate	Closure of the School, plus 40 years	Securely disposed of
Asset management		
Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
Accounts and statements including budget management		
Annual accounts	Current academic year, plus six years	Disposed of against common standards

Loans and grants managed by the School	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of
Contract management		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Securely disposed of
All records relating to the monitoring of contracts	Current academic year, plus two years	Securely disposed of
Banking		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of
School meals		
Free school meals registers	Current academic year, plus six years	Securely disposed of
School meals registers	Current academic year, plus three years	Securely disposed of
School meals summary sheets	Current academic year, plus three years	Securely disposed of

9. Retention of other school records

9.1. The table below outlines the School's retention periods for any other records held by the School, and the action that will be taken after the retention period, in line with any requirements.

9.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Property management		
Plans of property belonging to the School	For as long as the building belongs to the School	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the School	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of School premises	Current financial year, plus six years	Securely disposed of
Maintenance		
All records relating to the maintenance of School carried out by contractors	Current academic year, plus six years beyond the period of guarantee	Securely disposed of
All records relating to the maintenance of School carried out by School employees	Current academic year, plus six years	Securely disposed of
Operational administration		
General file series	Current academic year, plus five years	Reviewed and securely disposed of
Records relating to the creation and publication of the School brochure and/or prospectus	Current academic year, plus three years	Disposed of against common standards
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus one year	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year plus one year	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year, plus six years	Reviewed then securely disposed of
Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Current academic year, plus six years	Reviewed then securely disposed of

Central government		
OFSTED reports and papers	Life of report then review	**Secure disposal**
Returns made to central government	Current year plus six years	Secure disposal
Circulars and other information sent from central government	Operational use	Secure disposal

10. Storing and protecting information

10.1. The DP Officer will undertake a risk analysis to identify which records are vital to the School's management and these records will be stored in the most secure manner.

10.2. The Admin/ICT Team will support and assure the operation of an effective back up system to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data for the purpose of compliance with the principle of integrity and confidentiality under the GDPR and business continuity. Backups of data must be made on a regular basis in accordance with the School's ICT infrastructure.

10.3. Where possible, backed-up information will be stored off the premises, using a backup service which is operated by a provider who is compliant with the GDPR.

10.4. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access only to those personnel who require access to fulfil their delegated duties in accordance with their job role.

10.5. Confidential paper records including records containing personal information are not left unattended or in clear view when held in a location with general access.

10.6. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.

10.7. Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.

10.8. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.

10.9. All electronic devices (including portable devices) are password-protected to protect the information on the device in case of theft.

10.10. Where possible, the School must enable electronic devices to allow the remote blocking or deletion of data in case of theft.

10.11. Staff and governors do not use non-encrypted personal laptops, computers, phones or other electronic devices for School purposes, which involve the downloading or storing of personal identifiable or confidential data.

10.12. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

10.13. Emails containing sensitive, personal or confidential information are encrypted or password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a secure and appropriate format.

10.14. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

10.15. Fax must not be used to send confidential, personal or sensitive information. More secure means must be sourced to send the data.

10.16. Where personal, sensitive or confidential information is taken off the premises, to fulfil the purpose of the protection of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow adequate procedures for security, e.g. USB drives are encrypted, paper documentation is kept in a locked, secure location which is not accessed by others. The person taking the information from the premises accepts full responsibility for the security of the data in accordance with this policy sections 10.17 and 10.18.

10.17. Where personal, confidential or sensitive data is removed from the premises, this must be agreed by the Executive Headteacher, on a temporary basis, and returned to the school within a time frame defined as acceptable by the Executive Headteacher. The personal, confidential or sensitive data will be removed in a format which is acceptable according to its original state, e.g. larger volumes of paper documentation such as exercise books are likely to be taken in their original format for marking purposes. Paper documentation must be kept secure at all times. During transportation, the method of transportation must be secure and the documentation must not be left unattended at any time. When stored off site, paper documentation must be maintained in a locked facility which is only accessible by authorised School personnel. All documents which are removed from the premises in a portable electronic format must be based on a portable electronic device which is encrypted. Data stored on encrypted hard drives or USBs must not be stored on or downloaded to personal devices.

10.18. All documents which are accessed by employees externally to their premise via a portable electronic device must be done so utilising designated School services such as the Cloud and Office365. Personal accounts must not be used to access School data. Data which is accessed 'off premise' via School email, cloud or remote desktop services must not be downloaded to or stored on personal devices, directly or indirectly, unless is it anonymised.

10.19. Before sharing data, staff always ensure that:

- They have a consent from data subjects to share it (where required).
- Data subjects have read and understood the privacy notice.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.
- The data shared is limited to what is necessary.
- The data shared is for specific and legitimate purposes.
- Arrangements are in place to ensure that the transfer of data to third parties is secure and the third party has sufficient security measures in place to be able to protect the personal data.
- They have verified the identity of the person requiring the data and that the person is entitled to receive the data.
- Telephone requests for data are vetted to confirm the identity of the person requesting the data and legitimacy for issuing it, including in accordance with Subject Access Requests.

10.20. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive, confidential or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

10.21. Personal data must not be stored on the hard drive of any device unless it is running appropriate encryption software.

10.22. Data must be subject to a robust password protection regime. Password sharing is not permitted and alternative means must be sought for sharing data.

10.23. Computers must be locked when not staffed to prevent unauthorised access.
10.24. Under no circumstances are visitors allowed access to confidential or personal information. Visitors accessing areas containing sensitive information are supervised at all times.
10.25. The physical security of the School's buildings and storage systems, and access to them, is reviewed **termly** (and documented) by the person with responsibility for sites in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Executive Headteacher and extra measures to secure data storage will be put in place. Data Protection Impact Assessments are undertaken where required.
10.26. Vital records should be stored in filing cabinets, drawers and cupboards which are raised (at least two inches from the ground in areas of fire or flood risks) to help mitigate the risk of theft, vandalism, fire and flood. Vital records should not be left on open shelves or desks.
10.27. Access to office where special category data is held should have restricted access.
10.28. Archive rooms should be lockable and secure, and be able to maintain restricted access.
10.29. Where lengthy retention periods have been identified as a requirement, consideration must be taken as to transferring paper records to an electronic media. Any data which is transferred into an electronic format should be legally admissible i.e. the School must be able to provide that the electronic version is a genuine copy of the original and not tampered with in any way.
10.30. The School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
10.31. The DPO is responsible for supporting continuity and recovery measures are in place to ensure the security of protected data.
10.32. Any damage to, theft or loss of data will be managed in accordance with the School's Personal Data Breach Management Plan.

11. Email Management

11.1. Email communication should be professional, clear and appropriate in nature in accordance with the School standards of communication.
11.2. Personal, sensitive and confidential data should only be sent by an encrypted email system.
11.3. Personal information should not be put into the subject line of an email.
11.4. Emails are disclosable under Freedom of Information and the GDPR legislation and therefore must comply with this.
11.5. Emails are not always deleted previously. Considerations must be made as to copies of the data held by recipients and the retention periods which must be implemented.
11.6. Emails can be classified as the format of a contract, entered into in writing. Individual members of staff may only enter into a contract if they have the appropriate authorisation to do so.
11.7. All email attachments which contain personal, sensitive or confidential data which require saving as opposed to viewing, must be downloaded onto suitable School devices and systems. Personal devices cannot be used to download or store email data. Printed attachments containing personal, sensitive or confidential data must be stored securely as outlined in section 10 of this policy.
11.8. Emails must be filed and deleted in accordance with this policy.
11.9. Staff must consider whether email communication is the most appropriate manner of communication in accordance with School standards of communication. Recipients must be limited only to those who absolutely require the information.

11.10. Emails containing personal, sensitive or confidential data must only be sent to an authorised email address. All emails used for School business must be sent to and from an official business domain address.

12. Accessing information

12.1. Shenstone Lodge School is transparent with data subjects, the information we hold and how it can be accessed.

12.2. All members of staff, parents of registered pupils and other users, e.g. visitors and third-party clubs, are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held (where the basis for processing the data requires consent).
- Understand what the School is doing to comply with its obligations under the GDPR.

12.3. All members of staff, parents of registered pupils and other users of Shenstone Lodge School and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.

12.4. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs. Under the UK derogation of the GDPR, the age of consent is 13. This information can still be shared with parents when pupils are aged 13 or over, where it is necessary to do so in order to fulfil the functionality or legal requirements of the School, the vital requirements of the pupil or in the absence of former reasons, where the pupil provides consent to do so.

12.5. Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

12.6. The School will adhere to the provisions outlined in the Shenstone Lodge School GDPR Data Protection Policy, Privacy Policy and the Procedure for Subject Access Requests when responding to requests seeking access to personal information.

13. Digital continuity statement

13.1. Digital data that is retained for longer than six years will be named as part of a digital continuity statement.

13.2. The DPO will support in identifying any digital data that will need to be named as part of a digital continuity statement.

13.3. The data will be archived to dedicated files on a server, which are password-protected – this will be backed-up in accordance with section 10 of this policy.

13.4. Memory sticks will never be used to store digital data, subject to a digital continuity statement.

13.5. The IT technician or equivalent will review new and existing storage methods annually and, where appropriate add them to the digital continuity statement.

13.6. The following information will be included within the digital continuity statement:

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats

- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the GDPR

14. Transfer of records to archives

14.1. Where records have been identified as appropriate for permanent preservation (in accordance with historical, scientific or statistical research purposes under the GDPR), the ICO must be consulted prior to undertaking the permanent preservation and a DPIA completed.

14.2. The School should document what records have been archived in this instance.

15. Information audit

15.1. The School will conduct an information audit on an **annual** basis against all information held by the Schools to evaluate the information the Schools are holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information

15.2. The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

15.3. The DPO is responsible for completing the information audit. The information audit will include the following:

- The Schools data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document

15.4. The DPO will consult with relevant staff members involved in the information audit process to ensure that the information is accurate.

15.5. Once it has been confirmed that the information is accurate, the DPO will record all details on the School's Information Asset Register.

15.6. The information displayed on the Information Asset Register will be shared with the SLT to gain their approval.

16. Disposal of data

16.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

16.2. Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The DP administrators will keep a record of all files that have been destroyed, how, when and by whom.

16.3. All records containing personal information or information which is sensitive/ confidential must be disposed of in a way which ensures they are unreadable or unreconstructable. Paper records must be shredded using a cross cut shredder, CDs/DVD, floppy disks should be cut into small pieces, audio/video tapes and fax rolls should be dismantled and shredded and hard drives must be wiped according to the nature of the data stored on them.

16.4. Where the School uses external providers to shred physical documentation or securely dispose of electronic hardware such as hard drives, records must be maintained as to the destruction alongside the company terms and conditions and contract for processing. Records must be made and retained upon the erasure of any original documentation, based electronically or in physical format.

16.5. Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.

16.6. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

16.7. Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

16.8. Where information must be kept permanently, this information is exempt from the normal review procedures

17. Monitoring and review

17.1. This policy will be reviewed on an annual basis by the DPO – the next scheduled review date for this policy is July 2019.

17.2. Any changes made to this policy will be communicated to all members of staff and the Chair of Governors.