

# Sheringham Woodfields School

Sheringham Woodfields School  
Holt Road  
Sheringham  
Norfolk  
NR26 8ND



JAMES STANBROOK  
Head Teacher

Telephone: 01263 820 520

Fax: 01263 820 521

Email: [office@sheringhamwoodfields.norfolk.sch.uk](mailto:office@sheringhamwoodfields.norfolk.sch.uk)

STEVE THURLOW  
Chair of Governors

Website: [www.sheringhamwoodfields.norfolk.sch.uk](http://www.sheringhamwoodfields.norfolk.sch.uk)

Registered Charity: Friends of Sheringham Woodfields School - 1127142

## DATA PROTECTION POLICY

Approved by SMT: 15 <sup>th</sup> March	Approved by Staff: 22 <sup>nd</sup> March	Approved by Governors: Spring 2021
Next Review date: Autumn 2023	Person(s) responsible for review: SLT	

Throughout this document we refer to Data Protection Legislation which means the Data Protection Act 2018 (DPA2018), the United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

This policy includes data retention arrangements, subject access requests and staff ICT usage/security arrangements. Given the nature of the school we do not feel it appropriate to ask pupils to sign an ICT usage/acceptance form. Instead they follow the schools E-Safety policy.

### 1. Aims

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 2018 and General Data Protection Regulations.

This policy applies to all data, regardless of whether it is in paper or electronic format.

### 2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 2018, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation in place.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

### 3. Definitions

Term	Definition
<b>Personal data</b>	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
<b>Sensitive personal data</b>	Data such as: <ul style="list-style-type: none"><li>• Contact details</li><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious beliefs, or beliefs of a similar nature</li><li>• Where a person is a member of a trade union</li><li>• Physical and mental health</li><li>• Sexual orientation</li><li>• Whether a person has committed, or is alleged to have committed, an offence</li><li>• Criminal convictions</li></ul>
<b>Processing</b>	Obtaining, recording or holding data
<b>Data subject</b>	The person whose personal data is held or processed
<b>Data controller</b>	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
<b>Data processor</b>	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

### 4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. The Governing Body and the Head Teacher are jointly responsible for this role.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually. The school is aware this requirement will change with the introduction of the GDPR in May 2018.

## **5. Data protection principles**

The Data Protection Act 2018 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

## **6. Roles and responsibilities**

The governing board has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 2018.

Day-to-day responsibilities rest with the headteacher, or the School Business Manager in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

The Data Protection Officer for the school can be contacted as follows:

**Name:** Matt Spall (DPO Centre)  
**Tel:** 01263 820520  
**Email:** [dpo@sheringhamwoodfields.norfolk.sch.uk](mailto:dpo@sheringhamwoodfields.norfolk.sch.uk)

## **7. Privacy/fair processing notice**

### **7.1 Pupils and parents**

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions
- Details of any Safeguarding concerns
- Details of any Behaviour(s) seen within school

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

Once our pupils reach the age of 13, we are legally required to pass on certain information to Norfolk County Council, which has responsibilities in relation to the education or training of 13-19 year-olds. Parents, or pupils if aged 16 or over, can request that only their name, address and date of birth be passed to Norfolk County Council by informing the School Business Manager.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

## **7.2 Staff**

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the School Business Manager.

## **8. Subject access requests**

Under the Data Protection Act 2018, all stakeholders have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The subject's name
- A correspondence address
- A contact number and email address
- Details about the information requested

Alternatively, a request can be made verbally in person or over the phone. If over the phone, verification of identity will still be required.

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days. The school may need to make a charge in connection with the cost of delivering said papers.

If a subject access request does not relate to the educational record, we will respond within 30 calendar days.

If you are unable to make this request in writing, please call the school on 01263 820520 and ask to speak to the Business Manager.

Proof of your identification will be needed for the subject access request to be actioned.

## **9. Parental requests to see the educational record**

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 13 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may not be granted without the express permission of the pupil.

If parents ask for copies of information, they will be required to pay the cost of making the copies.

## **10. Storage of records**

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use. All school provided laptops/devices will be encrypted.
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office and use one of the schools secure rucksacks.
- Passwords must be least 8 characters long containing letters and numbers (including upper case letters) are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment
- USB data/flash drives must not be used.
- Home/School diaries will be used to enable communication to take place between both school and home. Consent will be obtained to enable this to happen.

## **11. Disposal of records**

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. Please see Appendix A which details out the school retention of records policy.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

## **12. Training**

Our staff and governors are provided with data protection training as part of their induction process and via our e-learning suite of training.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

### **13. The General Data Protection Regulation**

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in May 2018.

We will continue to review working practices and provide training to members of staff and governors where appropriate.

### **14. ICT Systems within the school**

The school understands that ICT plays a very important part in the efficient running of the school. The school will:

- Provide devices for your sole use while you are a permanent full-time or part-time teacher at the school.
- Ensure devices are set up to enable you to connect to, and make effective use of, the school network.
- Ensure the relevant persons, such as the ICT Manager, have installed the necessary security measures on any school-owned device before your use - including, but not limited to, the following:
  - ✓ Firewalls
  - ✓ Malware protection
  - ✓ User privileges
  - ✓ Filtering systems
  - ✓ Password protection and encryption
  - ✓ Mail security technology
  - ✓ Tracking technology
  - ✓ Data encryption of all data stored on the school network

Ensure that all devices undergo the following regular checks and updates by the ICT Manager:

- ✓ Termly updates to malware protection
  - ✓ Termly software updates
  - ✓ Annual password re-set requirements
  - ✓ Termly checks to detect any unchanged default passwords
  - ✓ Malware scans in line with specific requirements
- 
- Plan and manage the integration of devices into the school environment, and provide the professional development required to enable you to use the devices safely and effectively.
  - When required, expect you to pay an excess for accidental damage or loss repair/replacement costs, where loss or damage is a result of your own negligence.

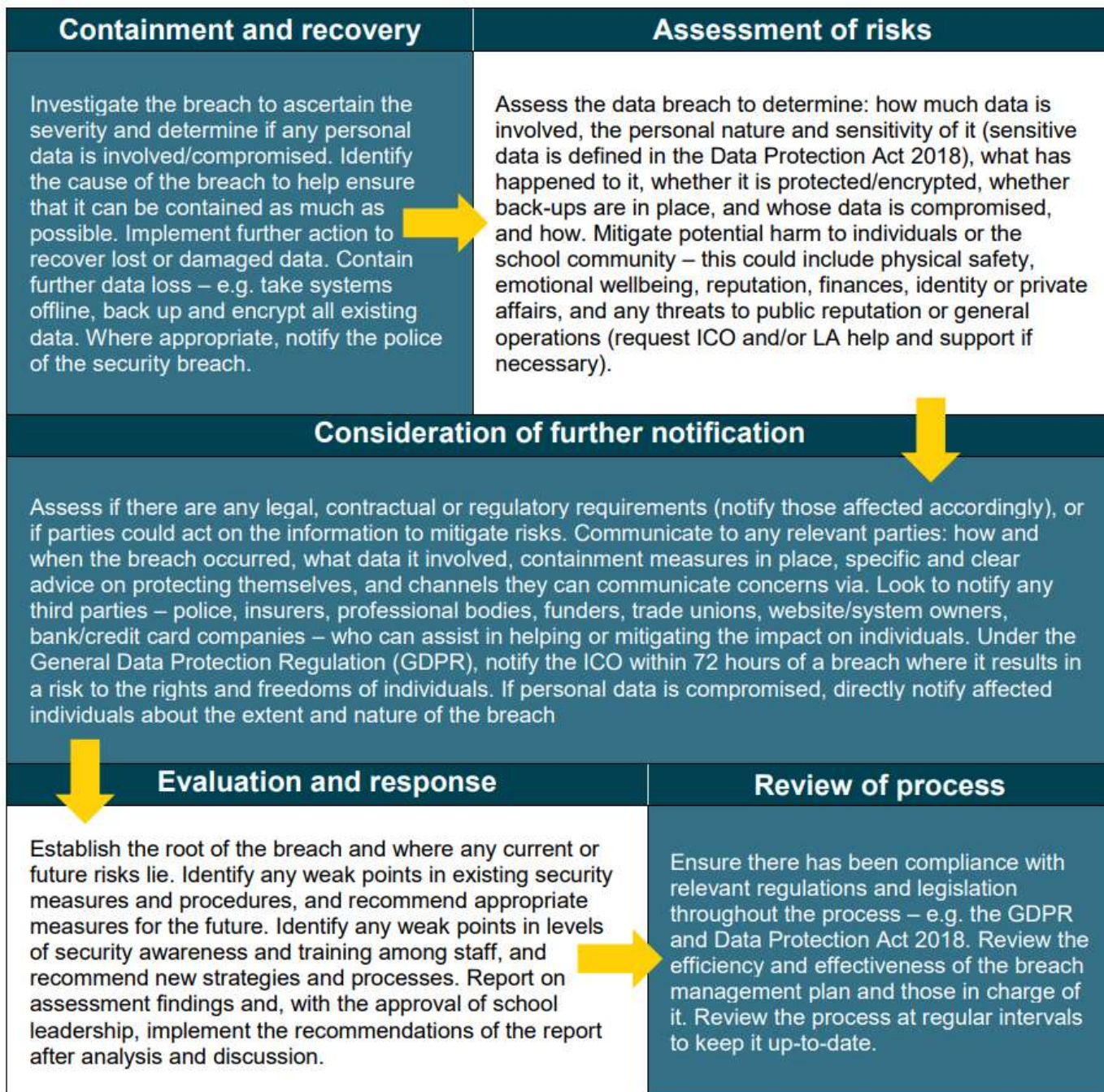
### **15. Data breaches**

It is hoped that with the robust systems in place, Data Breaches will be minimal, however the school understands that it has a duty of care to be able to record and respond to said breaches promptly.

All data breaches must be reported within 24 hours via the online form - <http://w.pfrms.co/e4ru4>  
The form feeds directly into the schools data breach log which only key members of staff have access to. All submissions will automatically go to the schools appointed DPO.

Below is the process the school and DPO will then take with regards to recorded breaches





## 16. Monitoring arrangements

The Senior Leadership Team are responsible for monitoring and reviewing this policy.

The School Business Manager checks that the school complies with this policy by, among other things, reviewing school records annually.

This document will be reviewed when the General Data Protection Regulation comes into force, and then every 2 years.

At every review, the policy will be shared with staff and the governing board.

## 17. Further reading

This policy should be read in conjunction with the following school based policies and documents:

- Safeguarding Policy
- Staff Handbook
- Mobile Phone Policy
- E-Safety Policy
- Personal Use of School Equipment Policy



## Appendix A

### Retention of Records Policy

This policy relates to both paper and electronic records across the school

Electronic records include:

- Files on the server
- Scholar Pack
- Tapestry and SPAT/SPT
- Pro-Forms

6.1 Governors					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Minutes					
<ul style="list-style-type: none"> <li>• <i>Principal set (signed)</i></li> </ul>	No		Permanent	Retain in school for 6 years from date of meeting	Transfer to Archives (could include archiving via GovernorHub)
<ul style="list-style-type: none"> <li>• <i>Inspection copies</i></li> </ul>	No		Date of meeting + 3 years	DESTROY [If these minutes contain any sensitive personal information they should be shredded]	
Agendas	No		Date of meeting	DESTROY	
Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives (could include archiving via GovernorHub)
Instruments of Government	No		Permanent	Retain in school whilst school is open	Transfer to Archives when the school has closed
Action Plans	No		Date of action plan + 3 years	DESTROY	
Policy documents	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Transfer to Archives

6.1 Governors					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes Destroy routine complaints	
Annual Reports required by the Department for Education and Skills	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years		Transfer to Archives
Proposals for schools to change its registration / type	No		Current year + 3 years		Transfer to Archives

6.2 Management					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Minutes of the Senior Management Team and other internal administrative bodies	Yes <sup>1</sup>		Date of meeting + 5 years	Retain in the school for 5 years from meeting	Transfer to Archives
Reports made by the head teacher or the SLT	Yes <sup>1</sup>		Date of report + 3 years	Retain in the school for 3 years from meeting	Transfer to Archives
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes <sup>1</sup>		Closure of file + 6 years	DESTROY If these records contain sensitive information they should be shredded	
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	DESTROY If these records contain sensitive information they should be shredded	

6.2 Management					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Professional development plans	Yes		Closure + 6 years	SHRED	
School development plans	No		Closure + 6 years	Review	Offer to the Archives

6.3 Pupils					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives
Attendance registers	Yes		Date of register + 3 years	DESTROY (including any electronic records)	
Pupil files	Yes				
<ul style="list-style-type: none"> <li>Primary</li> </ul>			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the LA Attendance Team	
<ul style="list-style-type: none"> <li>Secondary</li> </ul>			DOB of the pupil + 30 years <sup>1</sup>	SHRED	
Special Educational Needs files, reviews and SandI plans	Yes		DOB of the pupil + 30 year <sup>2</sup>	SHRED	
Letters authorising absence	No		Date of absence + 2 years	SHRED	
Absence records / diary	No		Current year + 6 years	SHRED	
Examination results	Yes				

<sup>1</sup> As above

<sup>2</sup> As above

6.3 Pupils					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
<ul style="list-style-type: none"> <li>Public</li> </ul>	No		Year of examinations + 6 years	DESTROY	Any certificates left unclaimed should be returned to the appropriate Examination Board
<ul style="list-style-type: none"> <li>Internal examination results</li> </ul>	Yes		Current year + 5 years <sup>3</sup>	DESTROY	
Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or DESTROY	
Statement maintained under The Education Act 1996 - Section 324 or EHCP	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	DESTROY unless legal action is pending	
Proposed statement or amended statement / proposed EHCP or amended EHCP	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	DESTROY unless legal action is pending	
Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	DESTROY unless legal action is pending	
Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	DESTROY unless legal action is pending	
Children SEN Files	Yes		Closure + 30 years	DESTROY unless legal action is pending	
Bio-metric eye gaze related data	Yes	Special Educational Needs and Disability Act 2001 Section 1	Delete profiles within 10 days of a pupil leaving the school	DESTROY	

<sup>3</sup> If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

6.3 Pupils				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Home/School diaries	Yes		To be destroyed within 1 term of pupil leaving the school OR to be given to the family to keep	DESTROY via SHREDDING

6.4 Curriculum				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Curriculum development	No		Current year + 6 years	DESTROY
Curriculum returns	No		Current year + 3 years	DESTROY
School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY
Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY
Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY
Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY
Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY
Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY
Examination results	Yes		Current year + 6 years	DESTROY [These records should be shredded]

6.5 Personnel				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SHRED
Staff Personal files	Yes		Termination + 6 years	SHRED
Interview notes and recruitment records (successful candidates) including warner interview notes where applicable	Yes		Termination + 6 years	SHRED
Interview notes and recruitment records (unsuccessful candidates) including warner interview notes where applicable	Yes		Interview date + 6 months	SHRED
Pre-employment vetting information (including DBS checks)	No	DBS guidelines	Date of check + 6 months	SHRED by a DSL if not required to meet Ofsted requirements
Disciplinary proceedings:	Yes		<b>Please note that all these retention periods where the warning relates to child protection issues may change in light of any recommendations made by the Richard Inquiry.</b>	
<ul style="list-style-type: none"> <li>Professional Advice and Guidance</li> </ul>			Termination + 6 years	SHRED If this is placed on a personal file, it must be weeded from the file.
<ul style="list-style-type: none"> <li>Oral warning</li> </ul>			Date of warning + 6 months	SHRED If this is placed on a personal file, it must be weeded from the file.
<ul style="list-style-type: none"> <li>written warning - level one</li> </ul>			Date of warning + 6 months	SHRED If this is placed on a personal file, it must be weeded from the file.
<ul style="list-style-type: none"> <li>written warning - level two</li> </ul>			Date of warning + 12 months	SHRED If this is placed on a personal file, it must be weeded from the file.
<ul style="list-style-type: none"> <li>final warning</li> </ul>			Date of warning + 18 months	SHRED If this is placed on a personal file, it must be weeded from the file.
<ul style="list-style-type: none"> <li>case not found</li> </ul>			DESTROY immediately at the conclusion of the case	
Records relating to accident/injury at work (OSHENS)	Yes		Date of incident + 12 years	Review at the end of this period. In the case of serious accidents a further retention period will need to be applied



6.5 Personnel				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Annual appraisal/assessment records	No		Current year + 5 years	SHRED
Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year +3 years	SHRED
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SHRED
Name, Role and Photo related information used to produce door access pass (swipe)	Yes		Delete within 10 days of the member of staff leaving the school	DESTROY physical card DELETE e-record

6.5 Health and Safety				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Accessibility Plans		Disability Discrimination Act	Current year + 6 years	DESTROY
Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		

6.5 Health and Safety					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
• <i>Adults</i>	Yes		Current year + 3 years	SHRED	
• <i>Children</i>	Yes		DOB + 30 years <sup>4</sup>	SHRED	
COSHH			Current year + 10 years	Review	
Incident reports	Yes		Current year + 20 years	SHRED	
Risk Assessments			Current year + 3 years	DESTROY	
Process of monitoring of areas where employees and persons are likely to have come in contact with <b>asbestos</b>			Last action + 40 years	DESTROY	
Process of monitoring of areas where employees and persons are likely to have come in contact with <b>radiation</b>			Last action + 50 years	DESTROY	
Fire Precautions log books			Current year + 6 years	DESTROY	

6.6 Administrative					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Employer's Liability certificate			Permanent whilst the school is open	DESTROY once the school has closed	
Inventories of equipment and furniture			Current year + 6 years	DESTROY	
General file series			Current year + 5 years	Review to see whether a further retention period is required	Transfer to Archives

<sup>4</sup> A child may make a claim for negligence for 7 years from their 18<sup>th</sup> birthday. To ensure that all records are kept until the pupil reaches the age of 30 this retention period has been applied.

6.6 Administrative					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
School brochure/prospectus			Current year + 3 years		Transfer to Archives
Circulars (staff/parents/pupils)			Current year + 1 year	DESTROY	
Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required	Transfer to Archives
Visitors' book			Current year + 2 years	Review to see whether a further retention period is required	Transfer to Archives
PTA/Friends of SWS			Current year + 6 years	Review to see whether a further retention period is required	Transfer to Archives

6.7 Finance					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Annual Accounts		Financial Regulations	Current year + 6 years		Offer to the Archives
Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	Transfer to Archives
Contracts					
<ul style="list-style-type: none"> <li>under seal</li> </ul>			Contract completion date + 12 years	SHRED	
<ul style="list-style-type: none"> <li>under signature</li> </ul>			Contract completion date + 6 years	SHRED	
<ul style="list-style-type: none"> <li>monitoring records</li> </ul>			Current year + 2 years	SHRED	
Copy orders			Current year + 2 years	SHRED	
Budget reports, budget monitoring etc			Current year + 3 years	SHRED	
Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SHRED	
Annual Budget and background papers			Current year + 6 years	SHRED	

6.7 Finance					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Order books and requisitions			Current year + 6 years	SHRED	
Delivery Documentation			Current year + 6 years	SHRED	
Debtors' Records		Limitation Act 1980	Current year + 6 years	SHRED	
School Fund - Cheque books			Current year + 3 years	SHRED	
School Fund - Paying in books			Current year + 6 years	SHRED	
School Fund - Invoices			Current year + 6 years	SHRED	
School Fund - Receipts			Current year + 6 years	SHRED	
School Fund - Bank statements			Current year + 6 years	SHRED	
Applications for FSM, UFSM, travel, uniforms, 16-19 Bursary etc			Whilst child at school	SHRED	
Free school meals registers (if operational)	Yes	Financial Regulations	Current year + 6 years	SHRED	
Petty cash records		Financial Regulations	Current year + 6 years	SHRED	

6.8 Property					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Title Deeds			Permanent	These should follow the property	Offer to Archives
Plans			Permanent	Retain in school whilst operational then	Offer to Archives
Maintenance and contractors		Financial Regulations	Current year + 6 years	DESTROY	
Leases			Expiry of lease + 6 years	DESTROY	
Lettings			Current year + 3 years	DESTROY	
Burglary, theft and vandalism report forms			Current year + 6 years	SHRED	
Maintenance log books			Last entry + 10 years	DESTROY	
Contractors' Reports			Current year + 6 years	DESTROY	

6.9 LA					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Secondary transfer information	Yes		Current year + 2 years	SHRED	
Attendance returns	Yes		Current year + 1 year	DESTROY	
Circulars from LEA			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives
CME1 forms	Yes		Date of leaving until the child reaches 30		

6.10 DfE					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
HMI reports			These do not need to be kept any longer		Transfer to Archives
OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required	Transfer to Archives
Returns			Current year + 6 years	DESTROY	
Circulars from DfE			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives

6.11 Careers related					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Service level agreements			Until superseded	SHRED	
Work Experience agreements			DOB of child + 30 years	SHRED	

6.12 School Meals					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Dinner Registers			Current year + 3 years	SHRED	

6.12 School Meals				
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
School Meals Summary Sheets			Current year + 3 years	SHRED
School Dinner Weekly banking reports			Current year + 6 years	SHRED



## Appendix B – Staff ICT Usage and Security procedure/approval

### *Sheringham Woodfields School Staff - Acceptable ICT Use Agreement*

To ensure that staff are fully aware of their responsibilities with respect to ICT use, they are asked to sign this acceptable use agreement.

- I understand that ICT Equipment and files are the property of the school and agree that my use must be compatible with my professional role.
- I understand that the school ICT systems may not be used for private purposes, without specific permission from the Head Teacher.
- I understand that use for personal financial gain, gambling, political purposes or advertising is not permitted.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras, email and social networking. I understand that I must not use my own personal equipment (i.e. camera, phone, recording equipment) within school to record / take photos without prior permission from the Head Teacher.
- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will not install any software or hardware without permission as the school needs to ensure GDPR compliance as well as network safety/compatibility.
- I will never disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system. Guest logins are available for visitors to use. Siblings must obtain a guest login if you wish them to use the computer network. Obtained via ICT Manager.
- I will take all reasonable precautions to secure data or equipment taken off the school premises.
- I will report any incidents of concern to the school Designated Safeguarding Lead (DSL) or e-safety Coordinator as appropriate. These are logged.
- I will ensure that all electronic communications are compatible with my professional role and cannot be misinterpreted. I understand that I will not interact with current pupils (those who attend the school) on social networking sites.
- I will promote safe use of ICT with the students that I work with and will help them to develop a responsible attitude to ICT use.
- I will respect copyright and intellectual property rights.
- Immediately report any viruses or reduced functionality following a download or access to a site, to the e-safety officer.
- I understand that electronic files (pictures, recordings, video) involving/including pupils **must never** be taken off site and used for private use (such as uploading onto social networking sites). Electronic files must not be shared with other parents/carers/visitors. These files are the property of the school.
- I will comply with the school's confidentiality policy with respect to electronic communications in terms of social networking, personal emails and text messages.
- Staff will not communicate personal details relating to school, staff, pupils, classes or events that have taken place via any form of electronic communication (as detailed above). Under no circumstances will pupils/staff names, initials or any other descriptor that could identify a child/staff member be used.
- I will not use memory cards (in cameras) as a long term storage option for photos. I will move photos onto the photo server weekly and delete photos from camera's. All portable devices to be stored in classrooms at the end of each day. No device will be taken off school without prior consent/permission from a member of the Senior Leadership Team.
- I will ensure all information obtained in connection with the school is securely stored. If any information / ICT hardware is lost or misplaced I will report this to the Business Manager as soon as possible. Files and folders need

to saved/stored in the correct location on the server. Staff are not to duplicate data and store them within their own network folders/drives.

- Computers and devices must be 'locked' or logged out when not in use. All computers and devices are to be turned off at the end of each working day.
- All staff will use ICT in accordance with the schools Data Protection policy.
- I will make arrangements to return devices and passcode to the ICT Manager if my employment ends or if I am away from the school for more than two weeks.
- Data will not be printed from Pro Forms / Scholar Pack / SPAT unless it is essential to carry out your duty.
- If I resign/leave our employment I will not attempt to access school based systems after my official leaving date (emails, SPAT, Pro Forms, Remote Server etc).
- Emotional outburst sent through electronic mail (email) about any person educated, employed or linked to the school is expressly forbidden.
- Documents containing personal identifiable information (PII) will not be attached to emails whenever possible and instead a secure solution such as Google Docs will be used to share links to files/folders.
- Never transmit any form of PII via email / text / secure transfer without first securing approval from a member of the leadership team.
- When receiving PII and other sensitive information via email, this should be transferred immediately (immediately defined as the point at which you open and read said email) into the necessary school system (i.e. printed out for a pupil file, passed onto the office/SLT, transferred onto the server etc). Said email should then be permanently delated from your email account.
- Emails should only be kept for a period of time deemed appropriate. As a generic rule of thumb, emails in your inbox should be cleansed/reviewed at least every 45 days.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

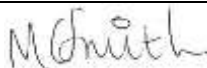
Insurance cover provides protection from the standard risks whilst the device is on the school premises or in your home but excludes theft from your car or other establishments. Should you leave the device unattended and it is stolen, you will be responsible for its replacement and may need to claim this from your insurance company or pay yourself.

Failure to agree to, or abide by, these terms will lead to the device being returned to the school and serious breaches may result in disciplinary action.

**Approved by member of staff:**

<b>Signed:</b>	
<b>Print name:</b>	
<b>Date:</b>	

**Approved by the school**

<b>Signed:</b>	
<b>Print name:</b>	<b>MR MATTHEW C SMITH</b>
<b>Date:</b>	