THE TOWERS

GDPR POLICY & DATA RETENTION POLICY

Approved by:	Governors – 10 December 2018
Ownership:	Head & operations Manager
Reviewed	October 2019
Next Review:	September 2020

Introduction

From the 25th May 2018 the General Data Protection Regulation (GDPR) was applicable.

This Policy sets out the manner in which personal data of staff, students and other individuals is processed fairly and lawfully.

The School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the School. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

The School is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The School must be able to demonstrate compliance. Failure to comply with the Principles exposes the School and staff to civil and criminal claims and possible financial penalties.

Aim

This Policy will ensure:

The School processes personal data fairly and lawfully and in compliance with the Data Protection Principles. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.

That the data protection rights of those involved with the School community are safeguarded.

Confidence in the School's ability to process data fairly and securely.

Scope

This Policy applies to:

- Personal data of all School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the School.
- The processing of personal data, both in manual form and on computer.
- All staff and governors.

The Data Protection Principles

The School will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The School will be able to demonstrate compliance with these principles.

The School will have in place a process for dealing with the exercise of the following rights by Governors, staff, students, parents and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including profiling.

Roles and Responsibilities

The Governing Body of the School and the Head are responsible for implementing good data protection practices and procedures within the School and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy

A designated member of staff, the Data Protection Officer, will have responsibility for all issues relating to the processing of personal data and will report directly to the Head in relation to the responsibilities of the Data Protection Officer role.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests, requests for rectification and erasure, data security breaches. Complaints about data processing will be dealt with in accordance with the Schools Complaints Policy.

Data Security and Data Security Breach Management

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All staff will comply with the School's E Safety & Safe Use of Technology. Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the E Safety & Safe Use of Technology.

Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Schools'.

New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment has been carried out.

The School will have in place a data breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) in compliance with the GDPR.

All staff will be aware of and follow the data breach security management process.

All staff will be aware of and comply with the list of Do's and Don'ts in relation to data security in Appendix A

Subject Access Requests

Requests for access to personal data - Subject Access Requests (SARs) will be processed by the Data Protection Officer. Those making a Subject Access Request will be charged a fee in accordance with Regulations. Records of all requests will be maintained.

The School will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time limit is one calendar month of receipt of the request.

Sharing data with third parties and data processing undertaken on behalf of the School.

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the School e.g. by providing cloud based systems or shredding

services, the School will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

Ensuring compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff.

All staff will read the E Safety & Safe Use of Technology.

The School advises students whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the School website.

The School also provides a Privacy Notice to staff which is available on the School website.

The School will ensure Privacy Notices contains the following information:

- Contact details for Data Controller and Data Protection Officer
- Purpose of processing and legal basis.
- Retentions period.
- Who we share data with.
- Right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.

Photographs, Additional Personal Data and Consents

Where the School seeks consents for processing person data such as photographs at events it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn.

Where the personal data involves a child under 16 years written consent will be required from the adult with parental responsibility.

To whom to report a data protection/GDPR issue/breach

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Fax: 01625 524 510

Appendix A

What staff should do:

DO get the permission of your manager to take any confidential information home.
DO transport information from school on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
DO use secure portable computing devices such as encrypted laptops when working remotely or from home.

DO ensure that all paper based information that is taken of premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.
DO ensure that paper based information and laptops are kept safe and close to hand when taken out of premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
DO return the paper based information to the School as soon as possible and file or dispose of it securely.
DO report any loss of paper based information or portable computer devices to your line manager immediately.
DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.
DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to SIMS (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic user names such as 'Sysman' are disabled.

What staff must not do:

DO NOT use unencrypted laptops
DO NOT use any external storage devices to store personal data
DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer/personal email.
DO NOT store work related documents on your home computer.
DO NOT leave personal information unclaimed on any printer or fax machine. **DO NOT** leave personal information on your desk overnight, or if you are away from your desk in meetings.
DO NOT leave documentation in vehicles overnight.
DO NOT discuss case level issues at social events or in public places.
DO NOT put confidential documents in non-confidential recycling bins.
DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.

Data Retention Policy for Personally Identifiable Information

1. Governing Body

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
Agenda for Governing Body meetings	Yes, if concerning confidential issues relating to staff		One copy to be retained with meeting minutes	Secure Disposal
Minutes of Governing Body meetings	Yes, if concerning confidential issues relating to staff		One copy to be retained with Agenda	Secure Disposal
Reports presented to the Governing Body	Yes, if concerning confidential issues relating to staff		Reports should be kept for a minimum of 6 years	Secure Disposal
Records relating to complaints dealt with by Governing Body	Yes		Date of resolution + 6 years	Secure Disposal
Log books of school activity, maintained by Head Teacher	Yes, if concerning individual pupils or staff		Date of last entry + 6 years	Secure Disposal
Minutes of Senior Leadership Team meetings (& other administrative bodies)	Yes, if concerning individual pupils or staff		Date of meeting + 3 years	Secure Disposal
Reports created by Head Teacher or SLT	Yes, if concerning individual pupils or staff		Date of report + 3 years	Secure Disposal
Correspondence created by staff	Yes, if concerning individual pupils or staff		Date of correspondence + 3 years	Secure Disposal
Professional Development Plans	Yes		Life of the plan + 6 years	Secure Disposal

2. Admissions Process

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
Admissions - if successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	Date of Admission + 1 year	Secure Disposal
Admissions – if unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels.	Last communication + 1 year	Secure Disposal
Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities	Date of Entry + 3 years	Secure Disposal
Proof of Address (as supplied by parents during admissions process)	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels.	Date of submission + 1 year	Secure Disposal

	Supplementary information		Yes		
For successful admissions	collected during admissions process (religion, medical conditions etc.)		Information should be added to the pupil file	Secure Disposal	
For unsuccessful admissions				Until process is completed	Secure Disposal

3. Operational Administration

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
Visitors' Books & Signing in Sheets	Yes		Current year + 6 years	Secure Disposal

4. Recruitment

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
All records leading up to the appointment of a new head teacher	Yes		Date of appointment + 6 years	Secure Disposal

All records leading up to the appointment of a new member of staff – unsuccessful candidate	Yes		Date of appointment of successful candidate + 6 moths	Secure Disposal
All records leading up to the appointment of a new member of staff – successful candidate	Yes		Transfer information to the staff personal file	Secure Disposal
Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide 2018: Keeping children safe in education. 2019 (Statutory Guidance from Dept. of Education) Sections 73, 74	School does not have to keep copies of DBS certificates. If copies are kept it must NOT be retained for any more than 6 months	
Proof of identity collected as part of the process of DBS check	Yes		Documentation should NOT be retained. Check and keep record of what has been checked. Add to staff file.	
Pre-employment vetting information: evidence proving the right to work in the UK	Yes	An employer's guide to right to work checks [Home Office May 2019]	Add documents to staff file (recommended). If held separately, keep for period of employment + 2 years	

5. Operational Staff Management

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
Staff Personal File	Yes	Limitation Act (1980)	Termination of employment + 6 years	Secure Disposal
Timesheets	Yes		Current year + 6 years	Secure Disposal
Annual appraisal	Yes		Current year + 5 years	Secure Disposal

6. Management of Disciplinary & Grievance Processes

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
Allegation of a child protection nature against a member of staff (including if unfounded)	Yes	"Keeping children safe in education Statutory guidance for schools and colleges 2019"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018"	Until normal retirement age or 10 years from date of allegation, whichever is longer.	Secure Disposal
Disciplinary Proceedings	Yes			
1. Oral warning 2. Written warning – L1 3. Written warning – L2 4. Final warning			1. Date of warning + 6 months 2. Date of warning + 6 months 3. Date of warning + 12 4. months Date of warning + 18 months	Secure Disposal
5. Case not found			Conclusion of case (unless Child Protection related)	

7. Health & Safety

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
Records relating to accident / injury at work	Yes		Date of incident + 12 years	Secure Disposal
Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
1. Adults 2. Children			1. Date of incident + 6 years 2. Date of incident + 25 years	Secure Disposal

8. Payroll & Pensions

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	Secure Disposal
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	Secure Disposal
PAYE	Yes	HMRC	Current year + 3 years	Secure Disposal

9.Pupil Management

Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Data Destruction
Pupil's Educational Record	Yes	Pupil Information Regulations 2005 *(note: not applicable for non-maintained schools)*		
1. Primary			Retain while pupil is at primary school	Pass to secondary school
2. Secondary		Limitation Act (1980)	Date of Birth + 25 years	Secure Disposal
Examination results	Yes		This information should be added to the pupil file and retained for current year + 6 years	Secure Disposal
SATS	Yes		Held in pupil file: Date of Birth + 25 years	Secure Disposal
Mark Books	No		Current year + 1 year	Secure Disposal
Pupil's work	No		Where possible, return to pupil at end of academic year	
Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges 2019"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018"	Any records should be in a sealed envelope and retained for the same period as the pupil file	Secure Disposal

Child Protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2019"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018"	Date of Birth of child + 25 years	Secure Disposal
Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities 2019	Date of entry + 3 years	Secure Disposal
Correspondence relating to authorized absence	Yes	Education Act (1996)	Current academic year + 2 years	Secure Disposal
Special Educational Needs files	Yes	Limitation Act (1980)	Date of birth of child + 25 years	Secure Disposal
Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act (2001)	Date of birth of child + 25 years (normally held on pupil file)	Secure Disposal