HILLSTONE PRIMARY

DATA RETENTION POLICY

The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

DATA PROTECTION

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the School. The School's Data Protection Policy outlines its duties and obligations under the GDPR.

RETENTION SCHEDULE

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule.

Paper records will be regularly monitored by Office Manager.

Electronic records will be regularly monitored by the Headteacher, in conjunction with the Strategic IT Manager.

The schedule is a relatively lengthy document listing the many types of records used by the school and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

DESTRUCTION OF RECORDS

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

ARCHIVING

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the Headteacher in conjunction with the relevant staff. The appropriate staff member, when archiving documents should record in this list the following information: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

TRANSFERRING INFORMATION TO OTHER MEDIA

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

RESPONSIBILITY AND MONITORING

The Headteacher has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The data protection officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD	DISPOSAL METHOD☐
Employment Records		
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained	Secure, confidential
Job applications and interview records of successful candidates	6 years after employment ceases	Secure, confidential
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases	Secure, confidential
Right to work documentation including identification documents	2 years after employment ceases	Secure, confidential
Immigration checks	Two years after the termination of employment	Secure, confidential
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.	Secure, confidential
Change of personal details notifications	No longer than 6 months after receiving this notification	Secure, confidential
Emergency contact details	Destroyed on termination	Secure, confidential
Personnel and training records	While employment continues and up to six years after employment ceases	Secure, confidential
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year	Secure, confidential

Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards	Secure, confidential
Disciplinary and training records	6 years after employment ceases	Secure, confidential
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.	Secure, confidential
Financial and Payroll Records		
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to	Secure, confidential
Statutory Sick Pay	3 years after the end of the tax year they relate to	Secure, confidential
Current bank details	No longer than necessary	Secure, confidential
Agreements and Administration Paperwork		
Collective workforce agreements and past agreements that could affect present employees	Permanently	Secure, confidential
Trade union agreements	10 years after ceasing to be effective	Secure, confidential
School Development Plans	3 years from the life of the plan	Secure, confidential
Professional Development Plans	6 years from the life of the plan	Secure, confidential
Newsletters and circulars to staff, parents and pupils	1 year	General waste
Staff codes of conduct	1 year	General waste
Health and Safety Records		
Health and Safety consultations	Permanently	Secure, confidential
Health and Safety Risk Assessments	3 years from the life of the risk assessment	Secure, confidential
Any reportable accident, death or injury in connection with work	For at least twelve years from the date the report was made	Secure, confidential
Accident reporting	Adults – 6 years from the date of the incident Children – when the child attains 25 years of age.	Secure, confidential

Fire precaution log books	6 years	Secure, confidential
Medical records and details of: - • control of lead at work • employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record	Secure, confidential
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made	Secure, confidential
Temporary and Casual Workers		
Records relating to hours worked and payments made to workers	3 years	Secure, confidential
Pupil Records		
Admissions records	1 year from the date of admission	Secure, confidential
Admissions register	Entries to be preserved for three years from date of entry	Secure, confidential
School Meals Registers	3 years	Secure, confidential
Free School Meals Registers	6 years	Secure, confidential
Special Educational Needs files, reviews and individual education plans (this includes any statement and all advice and information shared regarding educational needs)	Until the child turns 25.	Secure, confidential
Emails		
Other Records		
Any data or category of data which is not specifically noted above will be disposed of in a time frame to be determined by the Headteacher and added to this schedule as it arises.		