# The Croft Preparatory School

## Data Protection and Retention Policy

*Whole School Policy, including Early Years Foundation Stage*

| | |
|---|---|
| Reviewed (BT) | November 2022 |
| Peer Review Completed | 16 November 2022 |
| Ratified SLT | 22 November 2022 |
| Next Review Date | November 2024 |

The legal responsibility for ensuring that the Croft Preparatory School adheres to all relevant statutory regulations, as issued by the DfE, lies with the Proprietors. At their discretion, the Proprietors may delegate the monitoring of the efficacy with which the school discharges its statutory duties to the Compliance Manager and Governing Committee.

Notwithstanding the above delegation, the Proprietors retain ultimate responsibility for how the statutory functions are executed.

## General Statement of The Croft Preparatory School's Duties

During the course of the School's daily activities, personal data about staff, pupils, parents and third parties is collected, stored and processed. This personal data is sometimes sensitive in nature. The data is used in the ways outlined in the Privacy Notice.

All staff have a part to play in ensuring the school is compliant with its legal obligations under the Data Protection Act 2018 (DPA), incorporating the General Data Protection Regulation (GDPR), and those who are involved in the processing of personal data are obliged to comply with the procedures outlined in this policy. This policy may be amended at any time. Any update will be communicated via the normal school channels.

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (eg including parents, pupils and employees).

## Data Controller

The Croft Preparatory School is registered with the Information Commissioners Office (ICO) as a Data Controller of personal data.

## Data Protection Officer

Barney Thornton is currently acting as the Data Protection Officer (DPO), who will provide guidance to ensure that all personal data is processed in compliance with this Policy and the principles found in the Data Protection Act. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

## The Principles

The DPA 2018 sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and Data Processors, who process personal data on behalf of the Data Controller). These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specific and explicit purposes and only for the purposes it was collected for
3. Relevant and limited to what is necessary for the purposes it is processed
4. Accurate and kept up to date
5. Kept for no longer than is necessary for the purposes for which it is processed
6. Processed in a manner that ensures appropriate security of the personal data.

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

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

## Lawful grounds for data processing

At least one of these lawful grounds must apply whenever personal data is processed:

**(1) Consent:** the individual has given clear consent for us to process their personal data for a specific purpose (this consent can later be withdrawn however)

**(2) Contract:** the processing is necessary to fulfil the contract with the individual

**(3) Legal obligation:** the processing is necessary to enable the school to comply with the law

**(4) Vital interests:** the processing is necessary to protect someone's life

**(5) Public task:** the processing is necessary to perform a task in the public interest or for any official functions, and the task or function has a clear basis in law

**(6) Legitimate interests:** the processing is necessary for to enable the school to fulfil its legitimate interests

The lawful grounds for processing of personal data in School are outlined in the Privacy Notice, which is provided to all staff, volunteers, contractors, pupils and parents.

## DATA PROTECTION PROCEDURES

### Responsibilities of all staff

Record Keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that their personal data is inaccurate or untrue or if they are dissatisfied with the information in any way. Similarly, it is vital that the way they are recording the personal data of others – in particular colleagues, pupils and their parents – is accurate, professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that the originator would be able to stand by it if the person about whom it was recorded were to see it.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures. In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies and documentation:

- Data Protection and Retention Policy
- Information Security and Data Breach Policy
- Online Safety Policy
- Staff Code of Conduct

Responsible processing also extends to the creation and generation of new personal data/records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key obligations outlined in DPA (2018) regards the reporting of personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If a member of staff becomes aware of a personal data breach they must report it to the School's DPO. If staff are in any doubt as to whether or not to report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in serious consequences for the School, and for those affected, and could be a serious disciplinary matter whether under this Policy or the staff member's contract.

Care and data security

The School requires all staff to remain conscious of the six data protection principles (as outlined above), to attend any training required, and to use their best efforts to comply with the principles whenever processing personal information. Data security is not simply an online or digital issue but one that effects daily processes including creation and processing of hard copy documents.

We expect all those with management/leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the DPO, and to identity the need for (and implement) regular staff training.

## Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller. This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If a member of staff becomes aware of a subject access request (or indeed any communication from an individual about their personal data), they must tell the DPO as soon as possible.

Individuals also have legal rights to:

- require the Data Controller to correct the personal data held about them if it is inaccurate;
- request that their personal data is erased (in certain circumstances);
- request that data processing activities using their personal data are restricted (in certain circumstances);
- receive, from a Data Controller, the personal data held about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to a particular situation, to any particular processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw consent where it is being used as the legal basis for processing.

Except for automatic decision-making, none of these rights for individuals are unqualified and exceptions may well apply. In any event, however, if a member of staff receives a request from an individual who is purporting to exercise one or more of their data protection rights, they must tell the DPO as soon as possible.

## Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. As such, the following general principles apply:

- Staff must not use USB sticks/flash drives on the school site, nor email documents to personal email accounts to work on them from home. OneDrive and Sharepoint should be used to work on school documents remotely or collaborately.
- Staff members should lock their computer if they leave their desk, even if only for a few minutes
- Passwords should not be written down and never shared
- Use of personal email accounts for official school business is not permitted

The Information Security and Data Breach Policy provides more information on security protocols.

## Processing of Credit Card Data

The School complies with the requirements of the Payment Card Industry Data Security Standard (PCI DSS). Staff who are required to process credit card data must

ensure that they are aware of and comply with the most up to date PCI DSS requirements.

## Summary

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information fairly, lawfully, securely and responsibly.

The School's data protection policies and procedures are not intended to be oppressive, bureaucratic, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how to handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all staff and representatives are asked to be mindful of data protection and privacy issues. If in doubt, ask for help or assistance from the DPO.

**Data Retention Schedule**

The following table outlines the retention periods for data held by the School. Upon completion of the relevant retention period, the data should be destroyed in a secure manner. For the duration of the retention period, appropriate measures will be put in place to ensure the security of the data held.

| **Pupil Records** | **Retention Period** | **Status** | **Authority/Source** |
|---|---|---|---|
| Pupil records - including school admissions/registration documents, performance records and reports, pastoral information and medical records | DOB + 25 Years<br>(subject to safeguarding consideration where any material relevant to potential claims should be kept for the lifetime of the pupil) | Requirement | Limitation Act 1980/The Statute of Limitations (Amendment) Act 1991 |
| Accident/incident records pertaining to children | DOB + 25 Years | Requirement | Limitation Act 1980 |
| Special Educational needs records | DOB + 35 Years | Requirement | Allows for special extension to statutory limitation period |
| Records of any reportable death, injury, disease or dangerous occurrence | 3 years after the date on which it happened | Requirement | The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) |
| Examination results (internal or external) | 7 years from pupil leaving the school | Recommendation | ISBA |

| Early Years Records | Retention Period | Status | Authority/Source |
|---|---|---|---|
| Child's records - including admissions documents, pastoral information and medical records | DOB + 25 Years<br>(subject to safeguarding consideration where any material relevant to potential claims should be kept for the lifetime of the pupil) | Requirement | Statutory Framework for the Early Years Foundation Stage |
| Signing in sheets and registers | 3 years<br>(subject to safeguarding consideration where any material relevant to potential claims should be kept for the lifetime of the pupil) | Recommendation | Statutory Framework for the Early Years Foundation Stage |
| Early Years accident/incident records pertaining to children | DOB + 25 Years | Requirement | Limitation Act 1980 |
| Portfolio of work | To be sent home with the child | Recommendation | |

| Personnel Records | Retention Period | Status | Authority/Source |
|---|---|---|---|
| Personnel files and training records (including disciplinary records and redundancy details) | 6 years after employment ceases<br><br>NB do not delete any information which may be relevant to historic safeguarding claims | Recommendation | Chartered Institute of Personnel and Development (CIPD) |
| Records of Headteachers and School Proprietors | Permanently, for historical record | Recommendation | CIPD |
| Application forms and interview notes (for unsuccessful candidates) | 6 months | Recommendation | CIPD |

| | | | |
|---|---|---|---|
| DBS Check/Disclosure information | Schools…do not have to keep copies of DBS certificates in order to fulfil the duty of maintaining the single central record. Where a school or college chooses to retain a copy they should not be retained for longer than six months. | Recommendation | Keeping Children Safe in Education (KCSIE) April 2015 |
| Single Central Register | Keep indefinitely<br><br>Keep all checks retaining to current employees and leavers indefinitely | Requirement | As advised by Warwickshire Safeguarding Children's Board |
| Identity Documentation | A copy of the documents used to verify the successful candidate's identity, right to work and required qualifications should be kept for the personnel file. | Requirement | Keeping Children Safe in Education (KCSIE) April 2015 |
| Whistleblowing documents | 6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately. | Requirement | Public Interest disclosure Act 1998 and recommended IAPP practice |
| Working time records including overtime, annual holiday, jury service, time off for dependents, etc | 2 years from date on which they were made | Requirement | The Working Time Regulations 1998 |

| Safeguarding | Retention Period | Status | Authority/Source |
|---|---|---|---|
| Policies and procedures | Keep a permanent record of historic safeguarding policies | Recommendation | ISBA |
| Child Protection files | If a referral has been made/social care have been involved or a child has been the subject of a multi-agency plan – retain indefinitely<br><br>Low level concerns to be retained for 25 years from DOB.<br><br>Any doubt, retain indefinitely. | Requirement | ISBA |

| Pay Records | Retention Period | Status | Authority/Source |
|---|---|---|---|
| Payroll records (including overtime, bonuses and expenses) | 6 years | Requirement | Taxes Management Act 1970 |
| Statutory Maternity Pay (SMP) records | 3 years after the end of the tax year in which the maternity period ends | Requirement | The Statutory Maternity Pay (General) Regulations 1986 |
| Statutory Sick Pay (SSP) records | 3 years after the end of the tax year to which they relate | Requirement | The Statutory Sick Pay (General) Regulations 1982 |
| Income tax and National Insurance returns/records | At least 6 years after the end of the tax year to which they relate | Recommendation (The Requirement is 3 years) | The Income Tax (Employments) Regulations 1993 |

| | | | |
|---|---|---|---|
| National Minimum Wage Records | 3 years after the end of the pay reference period following the one that the records cover | Requirement | National Minimum Wage Act 1998 |

| **Health & Safety** | **Retention Period** | **Status** | **Authority/Source** |
|---|---|---|---|
| Risk Assessments | For as long as they are relevant and relate to a work activity, and then for an additional 6 years. | Recommendation | HSE |
| Staff accident books or accident records | 3 years after the date of the last entry (see below for records relating to an incident involving hazardous substances) | Requirement | Social Security (Claims and Payments) Regulations 1979 |
| Records of any reportable death, injury, disease or dangerous occurrence | 3 years after the date on which it happened | Requirement | RIDDOR 1995 |
| Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) 1999 | 40 years from the date of the last entry | Requirement | The Control of Substances Hazardous to Health Regulations 1999 and 2002 |
| Assessments under Health & Safety Regulations | Permanently | Recommendation | CIPD |
| Equipment monitoring and maintenance for safety purposes<br><br>(eg tallescope, electric gates, Mundell Court lift etc) | Life of the equipment + 6 years | Requirement | Limitation Act, 1980<br>The Provision and Use of Work Equipment Regulations 1998<br>The Lifting Operations and Lifting Equipment Regulations 1998 |

| | | | |
|---|---|---|---|
| Health & Safety General Training, including Instruction and training records, Material Safety Data Sheets, Safety Bulletins etc | 6 years after the material is superseded | | Limitation Act, 1980 |
| Fire Warden Training Evidence | 6 years | Requirement | Fire Precautions (Workplace) Regulations 1997 |
| First Aid Training Evidence | 6 years | Requirement | Health and Safety (First Aid) Regulations 1981 |
| Asbestos Inspections and Work | 40 years | Requirement | Control of Asbestos at Work Regulations 2002 |
| Fire Risk Assessment | 6 years after any new Fire Risk Assessment | Requirement | Limitation Act, 1980 |
| Emergency Planning/Crisis Management | 6 years after the material is superseded | Requirement | Limitation Act, 1980 |

| **Financial Records** | **Retention Period** | **Status** | **Authority/Source** |
|---|---|---|---|
| Accounting records, including Corporation Tax and VAT records and accounts | At least 6 years from the date on which they are made | Requirement | Section 386 of the Companies Act 2006 |
| Budget and internal financial reports | 3 years | Recommendation | ISBA |

| **Administration Records** | **Retention Period** | **Status** | **Authority/Source** |
|---|---|---|---|
| Complaints | Date of resolution of the complaint + 7 years | Requirement | |

| | | | |
|---|---|---|---|
| Annual Reports required by the DfE | Date of Report + 10 Years | Requirement | |
| Insurance liability documents | 40 years from date of issue | Requirement | The Employers' Liability (Compulsory Insurance) Regulations 1998 |
| Other Insurance documents | 6 years | Recommendation | |
| Minutes of meetings (Directors meetings, Governing Committee etc) | Signed copy to be kept permanently on file<br><br>other copies – date of meeting + 6 years | Recommendation | CIPD |
| Minutes, Notes and Resolutions of Boards or Management meetings | Minimum – 10 years | Requirement | |
| Certificates of Incorporation | Permanent (until dissolution of the company) | Requirement | IRMS |
| Register of members/shareholders | Retain permanently | Required | IRMS |
| Shareholder Resolutions | 10 years minimum | Recommendation | IRMS |
| Annual Reports | Date of report + 6 Years | Recommendation | IRMS |
| Signed final contracts and agreements | 7 years from completion of contractual obligations | Recommendation | |
| OSM Manuals and Building Documentation | Master copy to be kept for the lifetime of the building | Recommendation | |

| School Management | Retention Period | Status | Authority/Source |
|---|---|---|---|
| Registration documents of school | Permanent – until closure of the school | Recommendation | ISBA |
| Unsuccessful applications to the school and record of decisions | 12 months from application | Recommendation | ISBA |
| Attendance Register | 6 years from last date of entry, then archive | Recommendation | ISBA |
| Records documenting the development and planning of strategy – including School Development plans | 10 years | Recommendation | ISBA |
| Records documenting pupil numbers | 10 years | Recommendation | ISBA |
| Curriculum and planning | 3 years once superseded | Recommendation | ISBA |
| School Timetables | 1 year once superseded | Recommendation | ISBA |
| Assignment of pupils to classes, forms or sets | 1 year once superseded | Recommendation | ISBA |
| School's policies and procedures | 6 years once superseded | Recommendation | ISBA |
| Professional development plans and staff training materials | 6 years | Recommendation | ISBA |
| Correspondence, including email, created by the Headmaster and other members of staff with administrative responsibilities, for | 6 years | Recommendation | ISBA |

| | | | |
|---|---|---|---|
| issues where a formal record needs to be kept | (except where relevant to a safeguarding issue, where records must be held indefinitely) | | |
| School Magazine | Three copies to be kept indefinitely for historical purposes<br><br>All other copies to be destroyed 3 years after publication | Recommendation | |
| Staff Emails – sent and received | Emails containing personal data should be retained only for so long as required.<br><br>Any personal data received in emails that needs to be kept longer term should be filed in an appropriate location (eg Engage) and the email then deleted.<br><br>Sent emails containing personal data should be deleted from the 'sent item's' folder after the email has been sent | Recommendation | GDPR Auditing |
| Subject Access Request | 1 year following completion of the request | Requirement | Data Protection Act 2018 |
| CCTV Footage | 24 hours and then overwritten (required for any investigation in which case it should be kept for 6 months following the resolution.) | Recommendation | |

| School Photographs | Retention Period | Status | Authority/Source |
|---|---|---|---|
| Photographs of pupils and staff taken during the course of whole school educational activities, as part of class projects or homework<br><br>These may be used in class displays, pupil workbooks, or internal publications | To be deleted when the project is completed or at the end of the academic year (may be kept for an additional 12 months for inspection purposes)<br><br>Photos in workbooks to be sent home with the child at the end of the year<br><br>A proportion of these photos may be held in school indefinitely for the purposes of historical research | Recommendation | |
| Photographs of pupils or staff for use in school publications or external media (with permission) | To be deleted after inclusion in the publication. The publication to be retained as per above guidance | Recommendation | |

**Safeguarding**

Any material potentially relevant for safeguarding and child protection cases should be retained indefinitely. Data protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding claims.

**General Information**

Some types of records are not listed on the retention schedule. For example, records which are of little continuing value to the School which only need to be kept for a short period of time, ie hours, days or possibly weeks. They could be, for instance, telephone messages, written on pads or post-its; or handwritten or typed notes which are no longer needed or which have been transferred to a more formal document, which is being kept as a record.