

# Wickersley Kids Club

## GDPR-Compliant Records Management Policy

### Contents:

[Statement of intent](#)

1. [Legal framework](#)
2. [Responsibilities](#)
3. [Management of pupil records](#)
4. [Retention of pupil records and other pupil-related information](#)
5. [Retention of staff records](#)
6. [Retention of senior leadership and management records](#)
7. [Retention of health and safety records](#)
8. [Retention of financial records](#)
9. [Retention of other club records](#)
10. [Storing and protecting information](#)
11. [Accessing information](#)
12. [Digital continuity statement](#)
13. [Information audit](#)
14. [Disposal of data](#)
15. [Monitoring and review](#)

## Statement of intent

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

The club has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the club's statutory requirements.

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

Signed by:

\_\_\_\_\_ Bethany Eaton(Manager)

\_\_\_\_\_ Date: \_\_\_\_\_

\_\_\_\_\_ Hayley Green

Date: \_\_\_\_\_

## 1. Legal framework

- 1.1. This policy has due regard to legislation including, but not limited to, the following:
  - General Data Protection Regulation (2016)
  - Freedom of Information Act 2000
  - Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- 1.2. This policy also has due regard to the following guidance:
  - Information Records Management Society 'Information Management Toolkit for Clubs' 2016
- 1.3. This policy will be implemented in accordance with the following club policies and procedures:
  - Data Protection Policy · E-security Policy

## 2. Responsibilities

- 2.1. The Staff has a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.
- 2.2. The **Manager** holds overall responsibility for this policy and for ensuring it is implemented correctly.
- 2.3. **Bethany Eaton** is responsible for the management of records at **the club**.
- 2.4. The **Bethany Eaton** is responsible for promoting compliance with this policy and reviewing the policy on an **annual** basis, in conjunction with the **Deputy Manager**.
- 2.5. The **Manager** is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.
- 2.6. All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

## 3. Management of pupil records

- 3.1. Pupil records are specific documents that are used throughout a pupil's time at the club and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.(EYFS)

3.2. The following information is stored on the front of a pupil record, and will be easily accessible:

- Forename, surname, gender and date of birth
- Unique pupil number
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate

3.3. The following information is stored inside the front cover of a pupil record, and will be easily accessible:

- Ethnic origin, religion and first language (if not English)
- Any preferred names
- Position in their family, e.g. eldest sibling
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of parents, including their home address(es) and telephone number(s)
- Any other agency involvement, e.g. speech and language therapist

3.4. The following information is stored in about a pupil, and will be easily accessible:

- Admissions form
- Details of any special educational needs
- Annual written reports to parents (EYFS Children)
- Notes relating to major incidents and accidents involving the pupil
- Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan
- Any notes indicating child protection disclosures and reports are held
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health

- Notes indicating that records of complaints made by parents or the pupil are held

3.5. The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the **club office**:

- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
  - Correspondence with parents about minor issues, e.g. behaviour
6. Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the **clubs office** – a note indicating this is marked on the pupil's file.
7. Hard copies of complaints made by parents or pupils are stored in a file in the **Managers office** – a note indicating this is marked on the pupil's file.
8. Actual copies of accident and incident information are stored separately on the club's management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.
9. The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, **the Manager** responsible for disposing records, will remove these records.

10. The Club will not keep any copies of information stored within a pupil's record, unless there is ongoing legal action at the time during which the pupil leaves the club.
11. The club will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The club it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the club.

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

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

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

Type of file	Retention period	Action taken after retention period ends
<b>Admissions</b>		
Register of admissions	Three years after the date on which the entry was made	Information is reviewed and the register may be kept permanently
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Added to the pupil's record	Securely disposed of
<b>Pupils' educational records</b>		
Pupils' educational records (EYFS)	Whilst the pupil remains at the Club	

Child protection information held on a pupil's record	Stored in a sealed envelope for the same length of time as the pupil's record	Securely disposed of – shredded
Child protection records held in a separate file	25 years after the pupil's date of birth	Securely disposed of – shredded
<b>Attendance</b>		
Attendance registers	Last date of entry on to the register, plus three years	Securely disposed of

<b>SEND</b>		
SEN files, reviews and individual education plans	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the club to defend themselves in a 'failure to provide sufficient education' case
Statement of SEN maintained under section 324 of the Education Act 1996 or an EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEN	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold

Extra-curricular activities		
Parental consent forms for club trips where no major incident occurred	Until the conclusion of the trip	Up to 22 years after the pupil's date of birth
Parental consent forms for club trips where a major incident occurred	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	<b>Securely disposed of</b>
Walking bus registers	Three years from the date of the register being taken	Securely disposed of

## 5. Retention of staff records

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

Type of file	Retention period	Action taken after retention period ends
--------------	------------------	--

<b>Operational</b>		
Staff members' personal file	Termination of employment, plus six years	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of
<b>Recruitment</b>		
Records relating to the appointment of a new Manager	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
DBS certificates	Up to six months	<b>Securely disposed of</b>
Proof of identify as part of the enhanced DBS check	<b>After identity has been proven</b>	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, <b>securely disposed of</b>
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years	<b>Securely disposed of</b>

**Disciplinary and grievance procedures**

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

## 6. Retention of health and safety records

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

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

Type of file	Retention period	Action taken after retention period ends
<b>Health and safety</b>		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of

Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of <b>15</b> years is applied	Securely disposed of
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	25 years after the pupil's date of birth, on the pupil's record	Securely disposed of
Control of substances hazardous to health	Current academic year, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Securely disposed of
Fire precautions log books	Current academic year, plus six years	Securely disposed of

## 7. Retention of financial records

- 8.1. The table below outlines the club's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.
- 8.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Payroll pensions</b>		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
<b>Risk management and insurance</b>		
Employer's liability insurance certificate	Closure of the club, plus 40 years	Securely disposed of
<b>Asset management</b>		

Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
<b>Accounts and statements including budget management</b>		
Annual accounts	Current academic year, plus six years	Disposed of against common standards
Loans and grants managed by the Club	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of
<b>Contract management</b>		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Securely disposed of
All records relating to the monitoring of contracts	Current academic year, plus two years	Securely disposed of
<b>Club fund</b>		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of

## 8. Retention of other Club records

- 9.1. The table below outlines the Club's retention periods for any other records held by the club, and the action that will be taken after the retention period, in line with any requirements.
- 9.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
<b>Property management</b>		
Leases of property leased by the club	Expiry of lease, plus six years	Securely disposed of
<b>O p e r a t i o n a l administration</b>		
General file series	Current academic year, plus five years	Reviewed and securely disposed of
Records relating to the creation and publication of the club brochure and/or prospectus	Current academic year, plus three years	Disposed of against common standards
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus one year	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year plus one year	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year, plus six years	Reviewed then securely disposed of

--	--	--



## Storing and protecting information

10

- 10.1. The Manager will undertake a risk analysis to identify which records are vital to club management and these records will be stored in the most secure manner.
- 10.2. The Manager will conduct a back-up of information on an **annual** basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.
- 10.3. Where possible, backed-up information will be stored off the club premises.
- 10.4. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- 10.5. Confidential paper records are not left unattended or in clear view when held in a location with general access.
- 10.6. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.
- 10.7. Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.
- 10.8. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.
- 10.9. All electronic devices are password-protected to protect the information on the device in case of theft.
- 10.10. Where possible, the club enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- 10.11. Staff and governors do not use their personal laptops or computers for club purposes.
- 10.12. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- 10.13. Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.
- 10.14. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 10.15. When sending confidential information by fax, members of staff always check that the recipient is correct before sending.
- 10.16. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR,

---

either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the club premises accepts full responsibility for the security of the data.

- 10.17. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.
  - 10.18. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the club containing sensitive information are supervised at all times.
  - 10.19. The physical security of the Club's buildings and storage systems, and access to them, is reviewed **annually** by the **site manager** in conjunction with **the Manager**. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Manager and extra measures to secure data storage will be put in place.
  - 10.20. The Club takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
  - 10.21. The Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.
  - 10.22. Any damage to or theft of data will be managed in accordance with be reported the Paul Brooks and the clubs Data Protection Officer.
-

## 11 Accessing information

- 11.1. Wickersley Kids Club is transparent with data subjects, the information we hold and how it can be accessed.
- 11.2. All members of staff, parents of registered pupils and other users of the club  
e.g. visitors and third-party clubs, are entitled to:
  - Know what information the Club holds and processes about them or their child and why.
  - Understand how to gain access to it.
  - Understand how to provide and withdraw consent to information being held.
  - Understand what the club is doing to comply with its obligations under the GDPR.
- 11.3. All members of staff, parents of registered pupils and other users of the Club and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.

11.4. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

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

11.6. The Club will adhere to the provisions outlined in the club's **GDPR Data Protection Policy** when responding to requests seeking access to personal information.

.

## Digital continuity statement

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

12.2. The Manager will identify any digital data that will need to be named as part of a digital continuity statement.

12.3. The data will be archived to dedicated files on the Club's Laptop which is password secured. A back up will be taken on a Memory stick & stored offsite in a fire proof safe.

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

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the GDPR

## 13 Information audit

- 13.1. The club conducts information audits on an **annual** basis against all information held by the Club to evaluate the information the club is

holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

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

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

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

13.3. The Manager is responsible for completing the information audit. The information audit will include the following:

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

4. The Manager will consult with staff members involved in the information audit process to ensure that the information is accurate.
5. Once it has been confirmed that the information is accurate, **the Manager** will record all details on the Club's **Information Asset Register**.
6. The information displayed on the **Information Asset Register** will be shared with the Manager to gain their approval.

## 14 Disposal of data

- 14.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.
  
- 14.2. Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The Manager will keep a record of all files that have been destroyed.
- 14.3. Where the disposal action is indicated as reviewed before it is disposed, the Manager will review the information against its administrative value – if the information should be kept for administrative value, the Manager will keep a record of this.
- 14.4. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.
- 14.5. Where information has been kept for administrative purposes, the Manager will review the information again after **three** years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every **three** subsequent years.
- 14.6. Where information must be kept permanently, this information is exempt from the normal review procedures

## 15 Monitoring and review

- 15.1. This policy will be reviewed on an **annual** basis by the Manager in conjunction with the Owner – the next scheduled review date for this policy is April **2018**.
- 15.2. Any changes made to this policy will be communicated to all members of staff .

Date Reviewed: 2/5/18

Managers Signature:

Deputy Managers Signature: