



Data Safeguarding Policy and Procedure

Latest Review: August 2023

Review cycle: 3 years

Next Review: August 2026



Wellspring Learning Community

Data Safeguarding Policy and Procedure

Contributors to the 2023 review:

Head of School – Kathleen Battah
Director of Learning and Teaching – Rita Zgheib
Director of Administration and Operations – Abir Makki
Registrar – Nemr Abboud
Head of IT - Layal Abou Chacra
Educational Technologist – Oussama Mahfouz
Educational Technologist – Salam Zahran
Legal Compliance Officer – Yorgo Abi Khalil
Senior Executive Assistant – Sereen Ajami

Related Policies:

Educational Technology Master Plan
Staff Handbook

Approvals - names and signatures:

Chairperson of the Board

Head of School

Wellspring Learning Community

Data Safeguarding Policy and Procedure

Table of Contents

A. Introduction.....	2
1. Wellspring Learning Community’s Mission Statement.....	2
2. Rationale, Purpose, and Scope	2
3. Definitions	2
B. Data Safeguarding Policy	3
1. Data Safeguarding Principles	3
2. Sharing the Data Safeguarding Policy and Procedure.....	4
3. Sharing Personal Information Relating to Students.....	4
4. Types of Data Collected at School	4
5. Disposal of Records	4
6. Prevention of Data Breaches	4
C. Data Safeguarding Procedure	5
1. Data Safeguarding	5
2. Processes Regulated by the Data Safeguarding Procedure	6
3. Key Principles of the Data Safeguarding Procedure	7
4. Training and Awareness Program.....	7
5. Compliance and Supervision of Compliance	7
6. Holding Data and Keeping It Up to Date	7
7. Disposal of Data.....	8
8. Sharing and Transfer of Personal Data	10

Wellspring Learning Community

Data Safeguarding Policy and Procedure

A. Introduction

1. Wellspring Learning Community's Mission Statement

Wellspring Learning Community aims to establish an inquiry-based learning environment in which students from diverse backgrounds are given every opportunity to optimize their social, emotional and academic capacities and talents. Our students will become confident, resourceful, creative, caring, responsible global and local citizens prepared to use their education to contribute in meaningful ways towards improving society, both locally and internationally.

2. Rationale, Purpose, and Scope

Wellspring Learning Community is committed to protecting its database and that of all its constituents/stakeholders in addition, third parties such as, contractors, suppliers, and others shall abide by this Data Safeguarding Policy and Procedure.

This Data Safeguarding Policy and Procedure applies to the preservation, safeguarding and processing of data related to all community members as well as all other school data. Its purpose is to assist the school in meeting its ethical and legal obligations, to explain those obligations to staff, and to inform them how their data will be handled.

The Data Safeguarding Policy and Procedure is the foundation of the school's compliance with the Lebanese Data Protection Law 81/2018 and any other related laws, decrees, conventions, and regulations, including but not limited to the EU (European Union) General Data Protection Regulation (GDPR).

Note: Under this Data Safeguarding Policy and Procedure, WLC will not be held accountable nor liable in case of any breach that occurs on data that was transferred to any third-party platform.

3. Definitions

For the purpose of this Data Safeguarding Policy and Procedure, the following terms shall have the following meaning:

3.1 Wellspring shall mean Wellspring Learning Community in its entirety, in both campuses (Mathaf and CCC), including staff and students.

3.2 GDPR: the GDPR shall mean the European Union (EU) General Data Protection Regulation 2016/679

3.3 Data: for the purpose of this Data Safeguarding Policy and Procedure, Data shall mean both Personal Data and Institutional Data.

- 3.4 Data Subject:** a person who can be identified by reference to their data such as a name, an identification number, location data, etc. A data subject may be a student at Wellspring, an employee at Wellspring, supplier representative, a person applying for a job at Wellspring or subscribing to information by entering information on Wellspring's website.
- 3.5 Institutional Data:** any information gathered, processed, analyzed, and published by Wellspring in support of its overall mission to serve its members. Institutional data are the property of Wellspring.
- 3.6 Data Controller:** the natural or legal body, e.g., IT Department and/or Administration, which determines the purpose and means of processing data.
- 3.7 Personal Data:** any information relating to any data subject. Personal data includes all types of information that directly or indirectly may be linked to the data subject. Data may include:
- Personal information such as names, dates of birth, ID, passport details, contact details such as addresses, e-mail addresses, telephone numbers
 - sensitive personal information such as race, religion, ethnicity, political affiliation, etc.
 - information concerning salary and payment information
- 3.8 Data Breach:** shall mean any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data.
- 3.9 Processing:** any operation or set of operations performed upon the data, such as use, collection, recording, organization, structuring, adaptation or alternation, retrieval, storage, disclosure by transmission, or otherwise making available, restriction, erasure, or destruction.
- 3.10 Processor:** any person, authority, agency, or other body, which processes the data on behalf of the Controller, for example an outsourcing partner or service provider which processes data on behalf of Wellspring.
- 3.11 Transfer:** shall mean any data disclosure, copy, or move via a network, access from a system or web application or any data disclosure, copy or move from one medium to another.
- 3.12 Data Exporter:** any person who shares, transfers, or discloses data.
- 3.13 HOS Unit:** Head of School, Director of Learning and Teaching, Director of Strategic Development and Director of Administration and Operations.
- 3.14 LCO:** LCO shall mean Wellspring's Legal Compliance Officer.

B. Data Safeguarding Policy

1. Data Safeguarding Principles

The school complies with the principles of data Safeguarding set out under Lebanese Laws, which can be summarized as follows:

1. Information is obtained from the individuals themselves with full and informed consent.

2. Data will be kept accurate. Parents/guardians and staff should inform the school of any change which should be made to their Data to ensure that it is accurate, complete, and up to date.
3. Data will not be retained longer than necessary for the specified purpose for which it was given.
(See *Data Safeguarding Procedure Section 7: Disposal of Data*)

2. Sharing the Data Safeguarding Policy and Procedure

To emphasize transparency and build trust, this Data Safeguarding Policy and Procedure will be made accessible to all Wellspring staff and all community members on the school's website; it will also be shared with parents at the start of each school year.

3. Sharing Personal Information Relating to Students

During the application and admissions process, Wellspring obtains explicit consent from parents to share their children's personal data with their teachers and with third parties as well as their photos and/or videos for use in the school's publications, website or on social media.

Upon request, only names and grade levels of students will be shared with Wellspring's Parent Advisory Committee (WPAC). Like all other Wellspring stakeholders, WPAC is bound by the Data Safeguarding Policy and Procedure of the school.

4. Types of Data Collected at School

The following are examples of information collected about staff, students, and parents:

- contact information; photographs; health records
- student exams and exam results; attendance and behavioral information
- employees' records and staff appraisal reviews
- CCTV recordings and footage

5. Disposal of Records

Disposing of records will respect the retention period stated in detail in the Data Safeguarding Procedure for each type of data before it is safely deleted.

6. Prevention of Data Breaches

In case a data breach is suspected, it should be immediately reported to the LCO, who will follow up on the matter legally in accordance with the governing laws.

Security measures for data protection by preventing breaches include but are not limited to:

- holding telephone calls in public areas
- limiting access: only those who absolutely need to access the data should be able to
- shredding all confidential waste
- locking the information appropriately to avoid accidental access by others
- using firewalls and other filtering systems
- installing a security system and virus checker on computers; using strong passwords

C. Data Safeguarding Procedure

1. Data Safeguarding

Giving data subjects the ability to view and request changes to the information about themselves, such as names, phone numbers, preferences, etc., is a key component of data protection. The purpose of the safeguarding procedure is to guarantee that personal data processing is protected to a high standard.

The following data safety principles serve as the foundation for WLC's data safeguarding procedure:

- The collection of personal data shall only be done for specific, explicit, and legitimate purposes.
- The personal data shall be kept accurate and up to date.
- All personal data shall be kept confidential.

The LCO shall ensure that all stakeholders comply with the data safeguarding principles set out herein, and provide practical guidance to data subjects when concerned.

The institutional and personal data records held by the school may include:

- **Staff Records:**

Staff records will include, but not be limited to:

- personal data (name, address, phone number, emergency contact, medical records, etc).
- information about employment history
- any warnings or reports to authorities that the school have made regarding the staff member

- **Student Records:**

Student records will include, but not be limited to:

- personal information
- psychological, psychiatric, and/or medical exams and forms; individualized education plans.
- photographs of students; entrance exam results; records of behavioral/disciplinary issues from previous schools; previous academic records and assessments
- examination results, progress reports, and transcripts

- **Administrative Data**

Administrative data will include, but not be limited to:

- development-focused strategic plans
- operational rules and procedures
- student records pertaining to learning diversity
- behavior-related student records

- **Finance Data**

Finance data will include, but not be limited to:

- budgeting and projections; yearly reports and balances
- invoices and receipts
- compensation documents and tax records
- revenue and cash flow; assets and liabilities; and planning and projections.

2. Processes Regulated by the Data Safeguarding Procedure

Wellspring processes the following main categories of personal data concerning employees and students and their next of kin, clients, suppliers, contractors, visitors, joint ventures, and partners for the following main purposes (this table summarizes the above-mentioned data types):

Data category	Purpose of Processing
IT-administration data	Support and manage information technology (IT) and information system (IS) administration and information security.
HR management data	Recruitment, staffing, development of employees, talent management, succession planning, performance management and work force administration
Registrar data	Manage and process student's digital and physical data and history, registering/ up-dating students' records with the Ministry of Education and Higher Education (MEHE)
Student assessment data	Manage and process issuing, copying, and storing assignments, tests, exams, projects
Staff and students' health data	Manage and process medical information & Health Record; manage occupational health services and physical security, etc.
Audio and video recordings and related data	Internal and external communications, training and documentation through audio and video recordings.
Video surveillance/activity logs (e.g., CCTV footage and access logs)	Support/manage Safeguarding against illegal or unauthorized entry into areas, buildings, or rooms or to support the control of equipment and/or processes.
Data necessary to comply with legal obligations	Comply with legal obligations to which Wellspring is subject and/or protect a legal position of Wellspring.
Procurement data	Manage vendors selection, contracts and purchasing procedures

3. Key Principles of the Data Safeguarding Procedure

3.1 Data Subjects' Rights

All Data Subjects shall benefit from the rights to enforce:

- Lawful, fair, and transparent processing
- Data minimization, accuracy, and storage limitation
- Security and confidentiality
- Restrictions on onward transfers outside of WLC

Data Subjects' queries and complaints shall be handled in a timely manner by administration, the IT department, or the LCO depending on each query's specifics.

3.2 Liability

WLC has appointed its LCO to handle and resolve any damages resulting from the violation of the Data Safeguarding Procedure made by Data Subjects. Further, the LCO has the responsibility of taking necessary action to remedy the acts of such Data Subjects, and, where appropriate to impose compensation for any damages resulting from the violation of the Data Safeguarding Procedure by any Data Subject bound by the rules herein. The LCO shall liaise with outside counsel in case of a potential legal action.

4. Training and Awareness Program

Sharing the Data Safeguarding Policy and Procedure with new employees will be accomplished through a training program.

5. Compliance and Supervision of Compliance

The Legal Compliance Officer (LCO) shall have the following tasks:

- Handling local complaints from data subjects, related to the exercise of their individual rights
- General reporting and privacy issues reporting to the HOS Unit
- Following up on and monitoring changes in local laws and regulations and informing the HOS Unit when necessary
- Cooperating with the Ministry of Economy and Trade (MoET), and the local Data Protection Authority.

6. Holding Data and Keeping It Up to Date

During the time when WLC is holding personal data, the school will monitor for accuracy to ensure the data remains safe, relevant, and accurate.

The following procedures shall be carried out annually:

- Sending out a communication to parents and staff at the beginning of every school year requesting information updates, especially emergency contacts data.
- Checking that 'live' files are accurate and up to date.
- Amending data immediately without delay, as needed.
- Destroying any personal data that is out of date or no longer needed. This may involve shredding documents or deleting computer files securely so that they cannot be retrieved.

Parents whose children's applications are declined and job applicants whose applications are declined will be notified, in the decline letter, that WLC will retain their data in its systems and platforms unless requested by the parents or applicant to remove the information.

7. Disposal of Data

Data controllers shall follow the disposal of records schedules below, which state how long certain types of personal data can be held before they must be destroyed:

1. Students:

Record	Maximum Retention Period
Applications for enrolment/Transfer Forms	5 years after enrolment
Student Attendance Information/Registers	Date of Register + 10 years
Student Education Records (Reports etc.)	Until student is 23 years old
Student Records - School/Progress Reports etc. (Learning diversity needs)	Until Student is 26 years old
Child Protection Information: General	10 years after last entry on file
Child Protection Information related to Social Services investigation outcome substantiated	Until student is 30 years old
Disciplinary Actions	Until student is 23 years old
Timetables + Class Groupings Lists?	Retain while current
Examination Results	Current school year + 6 years
School trips; Financial/Administration details	Current fiscal year + 12 years
Reports of Stolen/Damaged Items	Current fiscal year + 6 years
Medical Records	Until student is 23 years old or in the case of a learning diversity student, until 26 years old

2. Staff:

Record	Maximum Retention Period
Personnel Records	10 years after leaving employment
Interview notes and recruitment records	Date of interview + 2 years 6 months
Salary Records	7 years after leaving employment
Sickness records	Current school year + 6 years
Substitute Teacher Records	Current school year + 6 years
Student Teachers (interns) on Teaching Practice – student teacher progress	Current school year + 6 years
Procedures for Induction of Staff	Until superseded
Staff/Teachers' Attendance Records	7 years after leaving (daily or contract)
Staff Performance Review	7 years after leaving

3. Administration:

Record	Maximum Retention Period
Governing Board – correspondence and meeting minutes	Current school year + 6 years
Senior Leadership and other staff meeting minutes	Current school year + 6 years
School Development Plan	10 years from closure of Plan
School Policies	as long as school is functional
Circulars to Staff, Parents and Students	Current school year + 3 years
School Brochure	as long as school is functional
Parents' Complaints	Until student is 30 years old
Annual Report	10 years from date of Report
Emergency Plans/Business Continuity Plans	keep different versions of policies as long as school is functional

4. Finance:

Record	Maximum Retention Period
Annual budget and budget deployment	Current fiscal year + 6 years
Budget Monitoring	Current fiscal year + 6 years
Annual Statement of Accounts	Current fiscal year + 6 years
Order Books, Invoices, Bank Records, Cash Books, Till Rolls, Log books etc.	Current fiscal year + 6 years
Postage Book	Current fiscal year + 6 years
Audit Reports	Current fiscal year + 6 years

5. Health & Safety:

Record	Maximum Retention Period
Accident Reporting (Adults) Employees	Date of incident + 7 years
Accident Reporting (Children) Students	Until student is 26 years old

Record	Maximum Retention Period
Risk Assessments – work experience	7 years
H&S Report reflections on practice drills	15 years
Fire Procedure	Until superseded
Security System File	For the life of the system

8. Sharing and Transfer of Personal Data

Transfer from Controller to Controller

Transfer of Data between Controllers and between Controllers and Processors may take place, provided that:

- it is compatible with the purpose for which the Personal Data were collected,
- it is in accordance with the principle of minimization, accuracy, and storage limitation,
- if applicable, information is given to the Data Subject,
- appropriate security measures protect the data during transfer/processing by the receiving Controller/Processor

Data Sharing - Platforms

The following table shows the platforms used by all staff at WLC along with the Data Types, owners and Permission Levels that are implemented:

Platform	Department	Data Type	Owner	Permission A*	Permission B*
Office 365	IT	Credentials; email addresses; calendars, etc.	IT Head	Educational Technologists	All other users
ManageBac	IT	Student records; Assignments/ Exams; Assessment	IT Head	HOS Unit; Principals; Coordinators; Registrar; Educational Technologists	Teachers Parents/Guardians
	Educational Technology	Transcripts; Lists; Analysis	Educational Technologists	HOS Unit; IT Head; Registrar; Educational Technologists; Principals; Coordinators	Teachers
OpenApply	Admissions	Enquiries; Applications; Requirements; Enrolment; Leavers	Director of Admission	HOS Unit; Registrar; Asst. Registrar; Educational Technologists	Coordinators; Exec. Assistants; Front desk
	Registrar	Synchronizing w/ eSchool; Reconciling	Registrar	HOS Unit; Registrar; Asst. Registrar;	Coordinators; Exec. Assistants; Front desk

Platform	Department	Data Type	Owner	Permission A*	Permission B*
		Application fees;			
eSchool	Registrar	Personal info; Requested documents	Registrar	HOS Unit Asst. Registrar; IT Head;	Teachers
	Finance	Student accounts; Student payments;	CFO; Director of Finance	Accounting	HOS Unit
MEHE	Registrar	Student lists & info; Student results; Official Exams lists;	Registrar	HOS Unit Asst. Registrar	
	HR	Staff lists & info	HR Coordinator	HR	
CERD (website)	Registrar	Student lists & info	Registrar	HOS Unit Asst. Registrar	
	HR	Staff lists & info	HR Coordinator	HR Support	
Follet Destiny	Libraries	Libraries Inventories Events Hold Lists	CCC Librarian	HOS Unit; Principals; Coordinators; Registrar; Asst. Librarian	
			Mathaf Librarian		

* Permissions:

A: Allow users to contribute (edit/change)

B: Allow users to view only

C: Allow to upload/download

The following table shows the student-related platforms used at Wellspring:

#	App Name	Description	Mathaf	CCC
1	Kamkalima	Arabic educational platform for learning and teaching		✓
2	Turnitin	Internet-based plagiarism detection service		✓
3	Britannica School	Citable, online learning resource		✓
4	Kognity	A curriculum-aligned teaching and learning platform with interactive content, analytics & assessment support		✓
5	InThinking	A comprehensive range of resources for new & experienced IB teachers		✓
6	Philpot	Supports IB teachers and students with online resources & workshop		✓
7	BrainPOP	Offers curriculum based animated movies, learning games, interactive quizzes, and a breadth of activities and resources	✓	
8	Destiny (by Follet)	Library management system for K-12 schools worldwide		✓

#	App Name	Description	Mathaf	CCC
9	Kutubee	An interactive reading platform that offers illustrated stories in Arabic for students to develop their reading skills	✓	
10	Mathletics	An online math program that transforms the way students learn math to build confidence through personalized learning, exciting games, and mastery challenges	✓	
11	Learning A-Z	An online guided English reading program with interactive eBooks, downloadable books, and reading quizzes	✓	
12.1	Raz-Plus	A blended platform that combines teacher-led whole-class and small-group instruction with technology-enabled resources for personalized reading practice.	✓	
12-2	Science A-Z	Thousands of resources in Life Science, Earth and Space Science, Physical Science, Engineering, and Process Science.	✓	
13	StoryboardThat	An online storyboarding tool that makes it easy to create a digital story in minutes using images, text, and templates.	✓	
14	Padlet	An online post-it-wall. It allows individuals to post their comments, questions, and resources in one place.	✓	
15	Twinkl	Provides instant access to teacher-created resources including worksheets, display materials, entire schemes of work, lesson planning and assessment materials	✓	
16	Scratch	A programming language and an online community where children can program and share interactive media such as stories, games, and animation with people all over the world	✓	

References

“Data Protection Act.”, *University of Bath*, 2023, www.bath.ac.uk/corporate-information/data-protection-act/.

“Data Protection Procedure: Processing and Transfer of Personal Data in Aker Solutions.”, *Aker Solutions*, 2018, www.akersolutions.com/globalassets/global/Data-Protection/Aker_Solutions_Data_Protection_Procedure_version_01.pdf.

“Data Protection Policy.” *Impact initiatives*, 2016, www.impact-initiatives.org/wp-content/uploads/2019/07/IMPACT-data-protection-policy_EN_2019_EN_v1.1.pdf