GSIF POLICIES, STANDARDS AND PROCEDURES

Information Technology

GOOD SHEPHERD INTERNATIONAL FOUNDATION ONLUS

GDPR REGULATION FOR THE USE OF IT EQUIPMENT[1]

TABLE OF CONTENTS

1.	**Introduction and purpose**
2.	**Scope of the policy**
3.	**Entry into force and distribution**
4.	**General principles on the use of the IT System**
4.1	**Ownership of the IT System**
4.2	**Personal use**
4.3	**Use of IT resources**
4.3.1	**General provisions**
4.3.2	**Use of portable devices**
4.3.3	**External memory devices**
5.	**User Accounts**
5.1	**Password management**
5.2	**Safeguarding authentication credentials**
6.	**E-mail**
6.1	**Personal use**
6.2	**Use and operation of e-mail**
6.3	**E-mail archive and retention time criteria**
7.	**Internet**
7.1	**Personal use**
8.	**Anti-virus protection**
9.	**Monitoring and controls**
10.	**Policy compliance and disciplinary procedures**
11.	**Right of access**

[1] *This chapter is an integral part of the GSIF GDPR (Global Data Protection Regulation) Policy.*

1. INTRODUCTION AND PURPOSE

The purpose of this policy (hereinafter, "**Policy**") is to establish the Foundation's procedures and rules on the appropriate use of **Good Shepherd International Foundation Onlus'** (hereinafter, the "**Foundation**") IT Systems, and to set out how data collected and processed by these systems is managed prudently and appropriately in line with national and EU legislation, in order to safeguard the Foundation's information assets and the IT security of the entire Foundation and protect them from accidental usage that may create problems or threats to the safety of IT systems and data processed.
For the purposes of this Policy the term:

- "**IT Systems**" means all computer or electronic equipment, mobile phones, e-mails, connections to electronic communication networks of any type (including internet access and online browsing) and by whatever means, software licensed to the Foundation for its use or any other purposes, personal computers (desktops, laptops and/or notebooks), workstations, portable devices (tablets, PDAs, notebooks, smartphones, external hard disks, USB flash drives, SIM cards, etc.) and any other type of support, service or anything else relating to the Foundation's IT infrastructure, owned or otherwise legally available for use by the Foundation, as well as any device connected to any of these, for whatever reason and by whatever means;
- "**IT Department**" means the Department made up of individuals who work as system administrators.

2. SCOPE OF POLICY

This Policy applies to all Users who are authorized to access the IT System including, by way of example but not limited to: employees - regardless of their role, qualifications and/or type of contract -, associates, consultants, temporary workers and any other third party authorized or given access to the IT System (the "**Users**").

3. ENTRY INTO FORCE AND DISTRIBUTION

This Policy shall enter into force on 18th December 2020. Recipients shall be made aware of this Policy by email. Any updates shall be distributed by the same means to facilitate communication and consultation with all Users who shall, therefore, be required to comply with it.

4. GENERAL PRINCIPLES ON THE USE OF THE IT SYSTEM

4.1 Ownership of the IT System

The Foundation owns[2] the entire IT System and everything concerning the allocation of workstations and IT resources constitute its patrimony. It is made available to Users for the sole purpose of carrying out the tasks assigned to them based on the employee/associate relationship. The attribution of ownership of the entire IT System to the Foundation shall also determine unless expressly stated otherwise - that all documents, material data and/or information that have been created, sent, received or stored in the IT System (including individual workstations) shall be regarded and treated by the Foundation as work-related and not confidential and/or personal in nature and, as such, aimed to the pursuit of the Foundation's corporate and institutional objectives, with resulting restrictions against it improper or unauthorized use.
If the employee/associate is redeployed or their contract is terminated, the User must not delete, alter or share confidential information owned by the Foundation, or any other type of information, without the express permission of the latter. In particular, without the express permission of the Foundation, the following activities are strictly forbidden and will be prosecuted by law:

- To provide third parties with access to the IT System.
- To delete files, information, software or licenses from the IT System.
- To make copies of files, information, software or licenses.
- To disclose or share internal information of any kind to third parties.

The Foundation gives permission for the IT system to be used for work purposes, on condition that the User agrees to be bound by this Policy and by any additional conditions that govern access to all confidential areas.

[2] *By owns is meant the Italian legal GDPR definition of "Titolarità".*

4.2 Personal use

Without prejudice to paragraph 6 below, the IT System shall be used for work purposes; however, occasional and limited use for personal purposes is permitted.

4.3 Use of IT resources

"IT resources" refer to all computing devices, such as desktops or portable personal computers, smartphones and tablets which are assigned to Users for work purposes (hereinafter "**Devices**").

4.3.1 General provisions

When using the Devices, the User must comply with the following rules:

I. Devices assigned to Users are work equipment, and each User shall be held responsible for the use of IT resources allocated to them. In particular, each User must use their Devices in a responsible, professional manner and in compliance with this Policy and all relevant national and EU laws and regulations concerning security.

II. All devices shall be installed with standard hardware and software which has been approved and purchased by the Foundation.

III. To prevent the risk of viruses being introduced or computer software being undermined, Users are not allowed to use software/hardware that originates from outside of the country; nor are Users permitted to use software with a shareware, free-to-try or free licence, without prior permission from the IT Department. In addition, any User who downloads any software without prior permission from the IT Department shall be held personally responsible for possible consequences on the Devices or in respect to third parties which result from its use.

IV. Do not connect hardware which has not been supplied by the Foundation or authorized by it in advance to Devices, except for input/output hardware such as a keyboard or mouse. Do not use USB flash drives or, in general, any removable device unless prior permission has been received from the Foundation; in which case a specific flash drive shall be assigned for data storage purposes, which has been subject to mobile device data encryption.

V. It is forbidden to modify or tamper with the hardware or software features of an assigned Device, or to transfer the standard hardware or software installed without prior permission from the IT Department.

VI. It is forbidden to use hardware or software tools designed to intercept, modify or delete the content of electronic computer communications and/or documents.

VII. The network drives are strictly to be used for only sharing work-related information and are not to be used in any way for any other purposes. Therefore, no file that is not work-related should be stored on these drives, even for short periods. The Foundation reserves the right to remove files or applications that pose a security risk to the system, or which have been acquired and installed in violation of this Policy.

VIII. Electronic communications within the Foundation must only be made through the Foundation's local or global area networks. Remote connections to the Foundation's network (either from a fixed or mobile network) are only permitted through the security standards put in place by the Foundation. Any other type of external connection to the Foundation's network is prohibited. If it is necessary, for work purposes, to connect to an external network other than through internal networks or network control standards, the connection must be made using a Device that is not connected to the Foundation's networks, subject to prior permission from the IT Department.

IX. All Users must save work-related data and/or documents on the Foundation's server/host.

X. It is strictly forbidden for assigned Devices to be used to share opinions that could be perceived as offensive or discriminatory (concerning gender, language, religion, race and ethnic origin, political opinion and/or trade union membership).

XI. It is strictly forbidden to attempt to access or use without permission any system, network or information owned by the Foundation, suppliers or third parties. It is also forbidden to attempt to probe the security of IT systems or networks or perform software piracy.

XII. It is forbidden to deliberately attempt to gain access to protected accounts, e-mails, documents or files, including tools to use software to obtain passwords or keywords (codes).

XIII. It is forbidden to install, create, introduce or replicate any computer virus or destructive code, logic bomb, worm, trojan horse, or other harmful software within the IT Systems. Moreover, if a User discovers a virus on their Device, they must immediately report this to the IT Department.

XIV. It is forbidden to attempt to access information contained in the files of other Users without the express permission of the Foundation, which will release this information in compliance with current legislation.

XV. It is forbidden to copy or reproduce computer software.

XVI. It is forbidden to use private cloud solutions – for example, Dropbox – to share the Foundation's data or documents. Where necessary, contact the IT Department to use the solutions available for this purpose.

4.3.2 Use of portable Devices

The use of portable Devices, such as smartphones, tablets, laptops, etc., may pose a risk to the Foundation of confidential information being disclosed or assets of considerable value being lost.

Without prejudice to the requirements set out in paragraph 4.3.1. above concerning portable Devices, please note, where appropriate, that the User is responsible for them and must safeguard them with due diligence both during travel and during use in the workplace. In particular, the User must safeguard them with the same care they take with their personal belongings. They must take all necessary precautions to prevent their damage or theft, for example, by not leaving portable Devices unattended in cars, trains or planes. If a portable Device is lost or stolen, the User must immediately inform the Foundation and the IT Department and, if requested, file a standard report to the competent authorities, a copy of which must be submitted to the Foundation.

In addition, the User must take care when using portable Devices in public places (e.g. at the airport, on the train, etc.), to prevent unauthorized third parties from viewing confidential work-related information.

Finally, please note that any portable Devices assigned to the User must only be used by them and therefore access to them by unauthorized third parties (family, friends, associates) is strictly prohibited.

4.3.3 External memory devices

"External memory devices" are defined as all devices that allow you to copy or store data, files or documents external to the personal computer. They include CD-ROMs, DVDs, USB flash drives, memory cards or keys, MP3 players, digital cameras, external hard drives, etc.

The usage rules set out in paragraphs 4.3.1. and 4.3.2. above are also applicable, where appropriate, to the use of external memory Devices.

External memory Devices containing confidential information and other information that constitutes corporate know-how must be treated with care and concern to prevent their contents from being stolen, altered and/or destroyed or, after having been deleted, recovered. All Users must take all necessary precautions to prevent against the risk of an external memory Device containing work-related information from being accessed without authorization, destroyed and/or rendered unusable.

Removable external memory devices are not permitted unless the User has obtained prior permission from the Foundation and has received a dedicated flash drive for data storage purposes. If permission has been granted, these Devices shall be subject to this Policy in the same way as if they were the Foundation's equipment or devices.

5. USER ACCOUNTS

Each User has their own account that allows them access to the IT Systems. Each account is personal, i.e. it is uniquely associated with the assigned User who shall be entirely responsible for all activities related to its use.

To access their account, each User must use their own username and password ("Authentication Credentials"), as set out in paragraph 5.1 below.

The Authentication Credentials to access the Foundation's network consist of a user ID associated with a confidential password.

The same user ID cannot be assigned to more than one person, even at different times. The User's Authentication Credentials will be disabled after six months of inactivity and/or if the User's employee/associate relationship with the Foundation is terminated.

5.1 Password management

Authentication Credentials to the Foundation's IT Systems are automatically allocated the first time the User connects to the system. When the User first connects to the system, a form will appear, and the User will be asked to enter their personal password. At this point, the User will then be prompted to replace it at once with a new password of their choice, consisting of a minimum of eight alphanumeric and special characters.

The User must keep their Authentication Credentials - and any other information relating to the authentication process - highly secret. In particular, they must never:

- disclose or share their password with anyone, including colleagues, friends or family;
- enter their password in the presence of unauthorized persons who may be able to view the details;
- write the password in an e-mail or on paper stored in the office.

The User must immediately change the password if there is any reason to believe that it has been revealed and report the issue to the IT Department or appropriate person.

5.2 Safeguarding authentication credentials

If a User is suddenly or for a prolonged period absent from work and/or unable, for whatever reason, to access their

electronic resources, the IT Department, namely the internal system administrator, shall be able to access the resources to create an out-of- office message. The IT Department will inform the relevant User about these actions as soon as possible.

6. E-MAIL

E-mail accounts assigned to Users are to be used for work-related purposes only; through which they can send and receive work-related messages, both internal and external to the Foundation (partners, suppliers, associates, consultants, etc.). As such, e-mail messages in the mailbox are not confidential and the Foundation may monitor these in compliance with the principles set out in paragraph 10.

6.1 Personal use

The e-mail account assigned to the User by the Foundation is exclusively to be used for work purposes only. Users shall be held responsible for the appropriate use of e-mail accounts assigned to them (Article 615-quater et seq. of the Criminal Code).
It is forbidden to use e-mail for anything other than work-related purposes. In addition, it is strictly forbidden to synchronize or combine the Foundation's account with a personal account or to back up the Foundation's e-mail on devices or for reasons other than for work purposes.
In particular, it is strictly forbidden to use e-mail to:

- share or forward 'chain letters' (messages with widespread and exponential circulation);
- send non-work-related generic requests (e.g. selling products and services);
- send unauthorized or offensive messages (including disparaging messages from colleagues or others), including text and/or images which may be perceived as illegal, inappropriate, pornographic or violent, racist or discriminatory (for reasons of gender, language, religion, race, ethnic origin, political opinion and/or trade union membership);
- participate in debates, chat forums or mailing lists for purposes other than work;
- participate in online auctions, competitions or games;
- exchange internal or external electronic communications with third parties which breaches the duties of loyalty, good faith and due diligence towards the Foundation or content which could damage its image or breach the duties imposed on each User by virtue of their relationship with the Foundation;
- send, receive or store material that violates copyright, trademark or other copyright or industrial property laws.

6.2 Use and operation of e-mail

Caution should be exercised with all e-mail received. To avoid the risk of being infected by viruses, e-mail received from unknown recipients or which appears unusual or contains suspicious attachments must be deleted before being opened. If in doubt, contact the IT Department for appropriate checks to be carried out.
E-mail attachments must be checked before they are used, and it is strongly advised not to download executable files or documents from unknown websites or FTP sites. Users must not disclose confidential information by any means, including by e-mail. It should be assumed that authorized individuals can access all electronic communication. Any documents belonging to the Foundation which are sent via e-mail must clearly indicate that the Foundation is the copyright holder.
In the event of planned absences (for example, for holidays or off-site work activities), the User must activate the automatic 'out of office' reply message available in the Foundation's IT System. The automatic reply must include contact details (including e-mail address or telephone number) of another User and/or other possible ways to contact the Foundation.
If an unplanned absence occurs (for example, illness) such that the User has not been able to activate the procedure outlined above, the Foundation can arrange to do this by informing the User concerned and in liaison with the IT Department.
In anticipation of a User being absent from work for a sudden or prolonged period, and of it being necessary to access the content of that User's e-mail messages for urgent work- related purposes, the IT Department shall be appointed as the User's delegate, unless notified to the contrary. In such way, the IT Department shall have permission to check the content of messages and to forward any messages deemed relevant for business continuity reasons to the data controller and/or to the person who made the request. A specific report on these actions will be will then be drawn up, and the User will be informed at the earliest opportunity. The User has the right to nominate a different person with permission to access their e-mail account by completing and submitting the trustee nomination form, attached **(Annex.1**).
If the employee/associate relationship is terminated, the IT Department shall immediately deactivate the User's e-mail

and activate a specific automatic reply message which shall notify third parties that the account has been deactivated. The account shall be deactivated in such a way as to permanently prevent the receipt of incoming messages addressed to the User's account, as well as their storage on the Foundation's servers.
At the end of the employee/associate relationship, the IT Department shall access the User's e-mail account to ensure the Foundation's business continuity and/or to protect the interests of the Foundation and shall prepare a specific report.

6.3 E-mail archive and retention time criteria

E-mail considered to be correspondence pertaining to the Foundation must be archived in the dedicated folders for that particular research project and/or in those relating to the administrative activity.
E-mails saved in this way shall be stored for one year since they are deemed to be business correspondence.
The Foundation shall delete e-mails from the User's e-mail account one year following the date on which they were sent or received.

7. INTERNET

Each User with a workstation has permission to browse the Internet. Particular attention shall be paid to Internet use and related services since all activity carried out is linked to the "Public IP Address" assigned to the Foundation and, in addition to the User, the Foundation shall be held liable (including criminal liability) for all sites visited and actions performed whilst browsing the Internet. All Users of the Internet must therefore act lawfully and responsibly.
The Internet can be used for work-related purposes authorized by the Foundation and in full compliance with the following rules. The Internet is a tool made available to Users for work purposes. Each User must therefore use the Internet in an appropriate and consistent way, aware that this access is assigned individually to the User to enable them to visit websites for work-related purposes, under the name of the Foundation.

7.1 Personal use

Complete access to the Internet is permitted for work purposes, and access is allowed for occasional personal use. Even for personal purposes, the laws in force must be respected, and the interests of the Foundation must not be prejudiced in any way, nor must profit- making or unethical intentions be pursued. In particular:

(i) It is forbidden to access specific categories of websites, such as pornography, child pornography, violence, malware, etc.

(ii) Unless expressly authorized by the Foundation, it is forbidden to upload or download free software (freeware and shareware) from the Internet, including the use of files (movies and music) from websites or HTTP sites unless strictly for work-related purposes and after having checked the trustworthiness of the sites in question (if in doubt, contact the IT Department).

(iii) It is forbidden to register on sites whose content is not work-related.

(iv) It is forbidden, other than for work-related purposes, to participate in forums, use online chats, electronic bulletin boards or register in guest books, even if using pseudonyms (or nicknames).

(v) It is forbidden to browse sites or store computer documents of an explicit, pornographic and/or discriminatory nature concerning gender, language, religion, race, ethnic origin, political opinion and/or trade union membership.

(vi) All files of uncertain or external origin, even if work-related, must be subject to an anti-virus scan.

(vii) It is forbidden to download and/or store large files except for work purposes and, in this case, after having sent them to the IT Department.

(viii) It is forbidden, for any reason, including not-for-profit, to share (for example, peer- to-peer) any audio-visual, cinematographic, photographic or IT materials, etc. which are protected by copyright, without prior permission from the Foundation.

(ix) It is forbidden to use the Foundation's logos or proprietary materials on any webpage or to publish them on the Internet, without prior permission from the operational unit or the Foundation's management.

(x) It is forbidden to access online gaming or betting sites.

(xi) It is forbidden to attempt to illegally obtain access, or cause damage or harm, to remote systems accessible via the Internet.

(xii) It is forbidden, other than for work-related purposes, to participate in forums, newsgroups, discussion groups or electronic bulletin boards.

(xiii) It is strictly forbidden to use the Internet for any purposes which are associated with the Foundation and which could portray it in a negative light or cause harm to it. As such, it is forbidden to carry out any activities (to share, download, save and/or connect) which may be considered illegal, fraudulent, unpleasant, disturbing, offensive, discriminatory or defamatory.

(xiv) It is forbidden to create websites on the Internet on behalf of the Foundation, through which to pretend to act on its behalf or to share data or information about it, in any way, without prior permission from the Foundation.

(xv) It is forbidden to publish the Foundation's electronic materials on computers which can be accessed via the Internet using anonymous FTP access or similar services, without prior express permission from the Foundation.

With regard to the previous paragraph and in accordance with the principles established therein, the Foundation, aware that social networks can play a role in creating and developing potential contacts to promote the institute, does allow Users limited use of these. To ensure that social networks are used appropriately, and in addition to the requirements set out in the previous paragraph, the User must also comply with the following rules:

I. Users in senior and managerial positions must not unless authorized to do so, provide recommendations and/or references on such sites concerning the Foundation's employees, associates, volunteers or former employees regarding current and/or past work performance. In general, all employees/associates/volunteers must assess the appropriateness of providing references on such sites.

II. Users must not disclose confidential and/or proprietary information belonging to the Foundation and must always avoid publishing unnecessary details regarding their professional activity.

III. It is forbidden to open "groups" or institutional or "corporate" pages on social networking sites in the name of the Foundation or on its behalf; nor must the Foundation's trademarks, documents and/or data and information be used for this purpose, without prior permission from the Foundation.

8. ANTI-VIRUS PROTECTION

To prevent access to non-work-related websites, the Foundation shall operate a specific automatic blocking or filtering system that prevents certain operations, such as uploading from, downloading to or accessing particular sites, included in a blacklist.

In addition, the Foundation's network is protected by anti-virus software which is automatically updated regularly. All Users must behave in a way that reduces the risk of the IT System being attacked by a virus or by any other aggressive software (for example, by not opening suspicious e-mails or their attachments, by only accessing corporate websites, etc.).

If any malware is detected by the anti-virus software, the User must immediately stop all current operations without turning the computer off and immediately report the incident to the IT Department.

Magnetic storage devices that originate from outside the Foundation (CDs, DVDs, pen drives, etc.) must be scanned by the anti-virus software before they are used and, if the software cannot remove a detected virus, the Device must not be used.

Publishing messages or information on the Internet can cause serious damage to the Foundation, given how rapidly information can be shared online. Therefore, the User shall be held personally responsible by the Foundation for any offensive, discriminatory or defamatory message published online and for any and all other illegal activities carried out by them.

9. MONITORING AND CONTROLS

Given that the entire IT System is aimed to facilitate Users to perform their business activities, information obtained and processed by the IT System may be used for all purposes related to the employment relationship, as set out in Article 4 of Law No. 300/1970 (the so-called "**Workers' Statute**"). Regarding this point, paragraph 10 below shall be invoked in full.

The Foundation reserves the right to carry out security checks and/or to check system functionality when failures or malfunctions occur, and to check that access to the Internet, e-mail and IT resources, and the use of the Foundation's IT System as a whole, is carried out in compliance with this Policy and current legislation.

These checks will be carried out in compliance with personal data protection legislation, in particular with regard to the provision of the Italian Data Protection Authority dated 1 March 2007, No. 13 which contains the "Guidelines for e-mail and Internet" (the "**Guidelines**"), and the principle of confidentiality of correspondence, as well as the rules on the protection of workers in accordance with Art. 2222 of the Civil Code (see Articles 4 and 8 of Law No. 300/1970).

In carrying out these checks, the Foundation will proceed according to the principle of 'graduality of the penalty'. As such, checks, where necessary, shall initially be carried out only on aggregated data referring to the Foundation in general or, where feasible, to entire offices, locations, sectors or networks and will conclude with a Foundation-wide notice or one limited to a specific office, location, sector or network. This notice shall contain, among other things, a request to scrupulously comply with this Policy. Should it be found that repeated breaches of the Policy occur, or there are signs of abuses or activities contrary to the duties imposed on the User by virtue of their employee/associate relationship, or if the anomaly that was initially detected should persist, it shall be possible to proceed with more specific and timely checks, even on an individual basis.

Such checks shall be carried out by the IT Department and/or by authorized consultants and, in compliance with the aforementioned legislation, they shall not be prolonged,ongoing or indiscriminate. In particular, the Foundation gives notice that it does not carry out systematic monitoring, such as, for example:

- Systematically read and record of e-mail messages or related external data, beyond what is technically necessary to provide the e-mail service.
- Systematically copy and subsequently store websites viewed by the employee.
- Reading or log characters typed into the keyboard or similar device.
- Secretly monitor laptops assigned for use.

Notwithstanding the above, if there are reasonable suspicions that the User has violated the terms of this Policy or if it is suspected that a crime has been committed, the Foundation - to protect its interests and in compliance with current legislation - reserves the right to access the IT System to obtain information relevant to the legal protection of its rights. In this event, any data or information obtained shall be stored solely for the use of judicial purposes and only for the time necessary for this purpose.

10. POLICY COMPLIANCE AND DISCIPLINARY PROCEDURES

All Users who use the IT System to perform their work activities shall be informed about any updates to this Policy or to the rules and regulations of applicable EU and Italian laws in force such as, among others, those concerning privacy (EU Regulation 679/2016, Legislative Decree 196/2003, as amended by Legislative Decree 101/2018, etc.), work safety (Art. 2087 of the Civil Code, Legislative Decree No. 81/08 and subsequent amendments, etc.), combating pornography and pedophilia (Arts. 600-*ter* and 600-*quater* of the Penal Code, Law 269/1998 and subsequent amendments, Law 38/06 and subsequent amendments, etc.), copyright protection (Law 633/1941 and subsequent amendments, etc.) and combating computer crimes (Arts. 615-*ter*, 615-*quater*, 615-*quinquies*, 635-*bis* and 640-*ter* of the Penal Code, Law No. 547/1993 and subsequent amendments, and Law No. 12/2012 and subsequent amendments, etc.). All Users, therefore, shall be held directly and personally responsible for their actions when using the IT System and, in general, work equipment assigned to them to carry out their tasks and duties, since their behavior may have an impact on the Foundation pursuant to Legislative Decree No. 231/2001 (Administrative liability of entities and companies).

If a User is found to have breached this Policy, the Foundation - in full compliance with the provisions of Art. 7 of Law No. 300/1970 and Italy's CCNL labor law - may apply disciplinary sanctions, such as, for example, verbal warnings, written warnings, fines, paid or unpaid suspension from work, and dismissal. Without prejudice to redress, including compensatory damages, and other punitive measures as stipulated by the provisions of civil and/or criminal law.

In addition, the Foundation shall - without the need for prior discussions and/or formal charges - immediately inform the competent authorities in the event of a crime being committed, whether actual or even only probable or suspected, as a result of unlawful or non-compliant use of the IT Systems.

11. RIGHT OF ACCESS

In accordance with the Guidelines and relevant legislation, Users are to be made aware that they can exercise their rights as "Data Subjects" - as set out in Article 15 and subsequently of the GDPR - by sending a request by e-mail to the Data Controller at the following address gsif@gssweb.org.

ANNEX 1

TRUSTEE NOMINATION FORM

I, the undersigned, [*insert name*] born in [*insert place]*, on [*insert date*], with Italian Tax Code No. [*insert number*] and resident at [*insert address*], in my role as an employee/associate of Good Shepherd International Foundation Onlus, with registered office in Rome, Via Raffaello Sardiello, 20, Italian Tax Code 97512090586, (hereinafter, for brevity, the "**Foundation**")

AUTHORISE

in accordance with the provisions of paragraph 5.2(b) of Resolution No. 13/2007 of the Italian Data Protection Authority, Mr/Ms [*insert name*] to carry out, in my name and on my behalf, the following operation:
to access the content of my e-mails, in the event of my sudden and/or prolonged absence from work, or for urgent business continuity reasons, and, after checking the content, to send the Foundation those messages relevant to perform the work-related activities, drawing up a specific report.

Rome, [*insert date*]

Mr/Ms [*insert name*]

SIGNATURE

_____

DATA BREACH NOTIFICATION MANAGEMENT[3]

TABLE OF CONTENTS

1. DEFINITIONS

2. INTRODUCTION

3. SCOPE OF THE DOCUMENT

4. DATA BREACH MANAGEMENT PROCESS

5. DATA BREACH CERTIFICATION

6. NOTIFICATION PROCEDURE

7. DATA BREACH PROCEDURE FLOW CHART

8. DATA BREACH NOTIFICATION FORM

1. DEFINITIONS

"**Personal Data"** means "*any information relating to an identified or identifiable natural person... in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" (Art. 4.1 of the GDPR).

"**Supervisory Authority**" means the "*Italian Data Protection Authority*".

"GDPR" means "*Regulation (EU) 2016/679 on the protection of personal data*".

"**Data Subject**" means the "*identifiable natural person... who can be identified, directly or indirectly, in particular by reference to an identifier*" (Art. 4.1 of the GDPR), for example, employees/associates, clients, suppliers, etc.

"**Notification**" means the Notification of a personal data breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it, [...] to the supervisory authority." (Art. 33.1 of the GDPR).

"IT Systems" means the computer or electronic equipment, mobile phones, e-mails, connections to electronic communication networks of any type (including the Internet and online browsing) and of any manner, software owned by the Foundation or licensed to it for its use or any other purposes, personal computers (desktops, laptops and/or notebooks), workstations, portable devices, (tablets, PDAs, notebooks, smartphones, external hard disks, USB flash drives, SIM cards, etc.) and in any other type of support, service or anything else relating to the Foundation's IT and communication infrastructure, owned or otherwise legally available for use by the Data Controller, as well as any device connected to it, *for any purpose and by whatever means.*

"**Authorized/Appointed Person***"* means a *"natural or legal person, [...] under the direct authority of the [Data] Controller or processor, [who is] authorized to process personal data*" (Art. 4.10 of the GDPR).

"**Data Controller**" is the "*Good Shepard International Foundation Onlus*".

"Processing" means "*any operation or set of operations which is performed on personal data or on sets of personal data, [...] such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Art. 4.2 of the GDPR).

2. INTRODUCTION

Herewith, **Good Shepard International Foundation Onlus** with registered office in Rome, Via Raffaello Sardiello 20, and with Italian Tax Code of 97512090586, details the procedure to notify the Supervisory Authority of a personal data breach to protect personal data and data subjects, pursuant to and in accordance with the provisions of Articles 33 and 34 of the GDPR.

[3] *This chapter is an integral part of the GSIF GDPR (Global Data Protection Regulation) Policy.*

3. SCOPE OF THE DOCUMENT

Article 4.12 of the GDPR defines a *"personal data breach"* as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed".*

As per Appendix B of the Guidelines published by ENISA on 4th May 2012, the nature of personal data breaches has been classified into six types which, hereinafter, for brevity, shall collectively be referred to as a *"***Data Breach***"*:

- Unauthorized or unlawful access: access to data by persons (internal or external to the Foundation) who do not have the right to do so.
- Loss: data being temporarily unavailable.
- Destruction: data being permanently unavailable.
- Transmission, processing, storing: (accidental or intentional) sharing of data to unauthorized recipients.
- Alteration or Modification: (accidental or intentional) alteration of data.
- Disclosure (e.g. to the public or unauthorized third parties): improper disclosure of confidential information.

By way of example, a typical Data Breach may consist of: a) the theft or loss of a desktop computer or portable device (for example, a laptop, removable disk, pen-drive, USB flash drive), b) external access to the Data Controller's data by a cyber-criminal/hacker; c) the accidental destruction or alteration of data and information; d) the disclosure of personal data to unauthorized persons; e) the loss or theft of paper documents; f) the public disclosure of personal data; g) viruses or other malicious attacks on the Data Controller's IT system or network, h) the breach of physical security measures such as, for example, forcing open doors or windows of particular rooms (i.e. rooms containing personal data files); i) accidentally sending e-mails containing personal and/or specific details to the wrong recipient; m) and, in general, any situation that could lead an unauthorized person having knowledge about or access to personal data.

The new regulatory provision of Art. 33 of the GDPR has introduced a number of obligations on the Data Controller, including the obligation to notify the Data Breach to the Supervisory Authority and, if a breach is likely to result in a high risk to the rights and freedoms of natural persons, to communicate this breach to the Data Subjects further.

The purpose of this document is to describe the operational procedures concerning these aforementioned obligations.

4. DATA BREACH MANAGEMENT PROCESS

All Authorized Persons involved in an alleged personal data breach affecting IT Systems that they and/or their Department, in general, use to carry out their work activities, must inform their line manager about the breach; senior management must directly notify the Director of Finance & Administration. This must happen as early as possible within eight hours, and under no circumstances later than 24 hours.

The Director of Finance & Administration, in liaison with the system administrator, shall investigate the information received in accordance with the provisions set out in paragraph
5 below and then report this to the head of the "General Management" department (hereinafter "**Director**").

Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, the Data Controller shall notify the Supervisory Authority of the data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. If it is necessary and/or required by the aforementioned legislation, the Data Controller shall also notify the Data Subjects about the breach. Where the Notification to the Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

5. DATA BREACH CERTIFICATION

In the event of the potential risk to the security of the Data Subjects' personal data, the Director of Finance & Administration, in liaison with the system administrator, shall begin an investigation to ascertain whether a Data Breach has occurred. Consequently:

a) If these investigations find the breach to be a "false alarm", the Director shall be informed and, following their permission, the incident shall be recorded.

b) If these investigations detect that an actual Data Breach has occurred, the Director shall be informed that:

- the process to notify the Supervisory Authority shall commence with immediate effect by sending an e-mail to the competent authority from the Data Controller's certified e-mail address, as more fully described in paragraph 5 below*;*
- if the breach has resulted in damage to the Data Subject's data or privacy, an assessment shall be conducted to determine if the Data Subjects need to be notified about the breach by reviewing the security measures in place on the IT Systems and data affected by the breach. For this assessment, the Data Controller shall take into account the criteria specified in the document "A*ssessment of the risks to the rights and freedoms of natural persons"* (**Annex 1**). Following this assessment, if the Data Controller still considers it necessary to notify

the Data Subjects, the most appropriate means of communication shall be identified.

In either case, whether hypothesis a) or hypothesis b) has occurred, the Director of Finance & Administration, in liaison with the Director, shall record the event in the "**Data Beach Register**", completing all necessary sections.

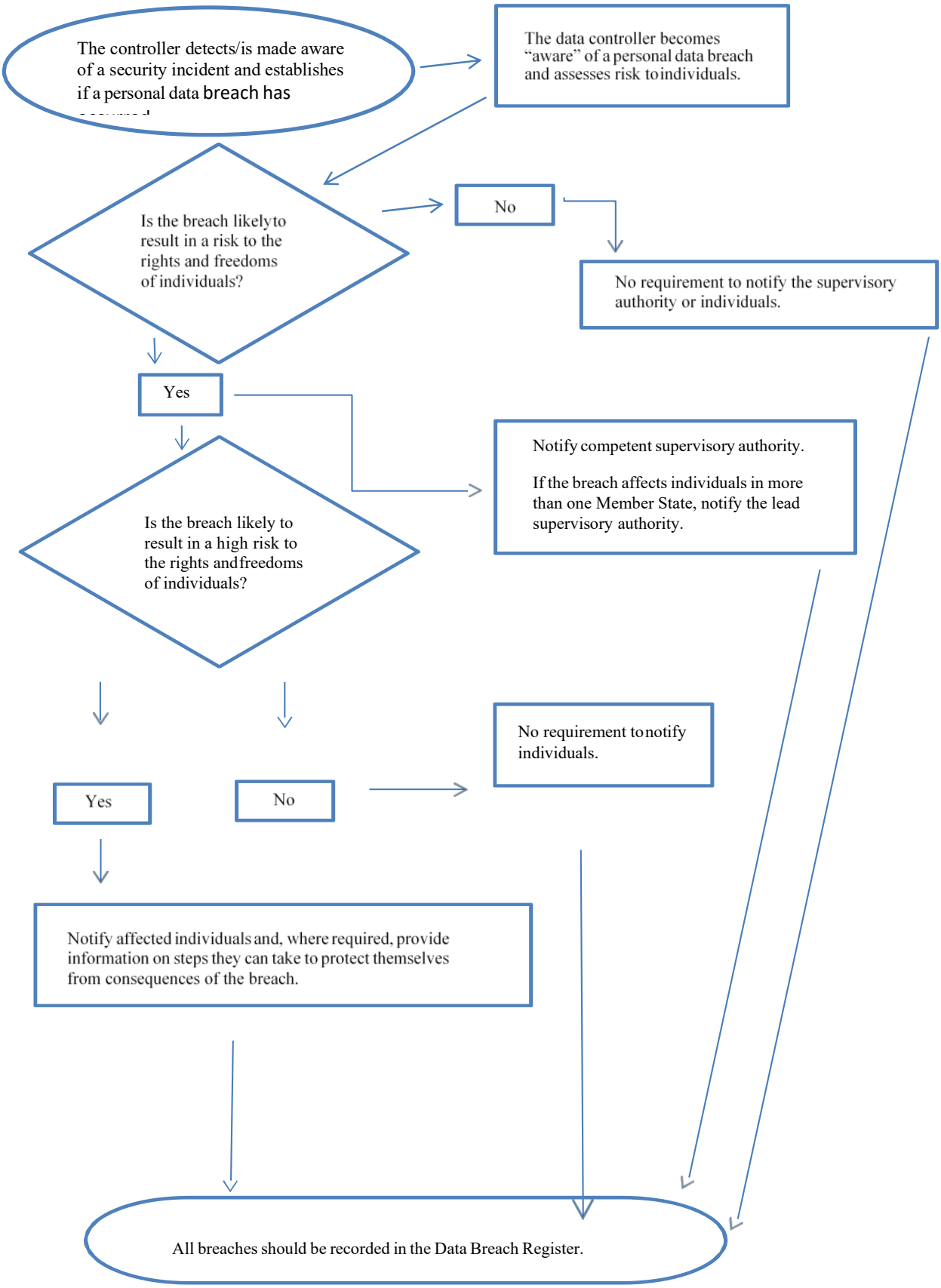
6. NOTIFICATION PROCEDURE

If the security incident has been certified as a Data Breach, the Data Controller shall complete, within the time specified by the legislation (i.e. not later than 72 hours after having become aware of the Data Breach), the Notification which must be sent to the Supervisory Authority using the form available on their website.
The Notification must contain the following information:

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
- The name and contact details of the contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.

- A description of the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to limit its possible adverse effects.

7. DATA BREACH PROCEDURE FLOW CHART



8. DATA BREACH NOTIFICATION FORM

Below is the form published by the Italian Data Protection Authority on 30th July 2019 to be used for the Notification of a Data Breach. Please check to see if there is an updated version available online, or if there is an online process to submit the Notification, on the Italian Data Protection Authority's website at the following address https://www.garanteprivacy.it/.

Notification type

○ Initial[1] ○ Comprehensive ○ Follow-up[2] Ref.

Carried out pursuant to ○ Art. 33 of the GDPR ○ Art. 26 of Leg. Decree 51/2018

Section A: Details of the person making the Notification

Surname: Forename:
E-mail:
Telephone:
Job title:

Section B: Data controller

Name of the organisation[3]:
Tax code/VAT No. No Tax code/VAT No. □
State:
Address:

Postal code: City: Province:
Telephone:
E-mail:
Certified e-mail address:

Section B1: Contact details for information about the breach

Provide the details of the contact person who can provide more information about this breach

o Data Protection Officer[4] - Prot. No.

o Other entity[5]

Surname: Forename:

1 The data controller initiates the notification process in the absence of a complete picture of the breach, subject to a subsequent follow-up notification. Sections A, B, B1 and C must be completed.

2 The data controller has previously submitted a notification (if known, enter the reference case file number assigned to the previous notification)

3 In the case of an individual, please enter the full name.

4 Where a DPO has been appointed, provide the relative protocol number assigned to their contact details.

5 In the absence of a DPO, provide the details of the designated contact point for the notification in question

E-mail:
Telephone:
Job title:

Section B2: Additional data processors

Please provide the details of other data processors involved and their role (joint controllers or processors[6], controllers' representatives based outside of the EU)

Name of the organisation[7]*:

Tax code/VAT No. No Tax code/VAT No. ☐

Role: ◦ Joint controller ◦ Processor ◦ Representative

Name of the organisation*: .....

Tax code/VAT No.: ..... No Tax code/VAT No. ☐

Role: ◦ Joint controller ◦ Processor ◦ Representative

Name of the organisation*: .....

Tax code/VAT No. ..... No Tax code/VAT No. ☐

Role: ◦ Joint controller ◦ Processor ◦ Representative

Name of the organisation*: .....

Tax code/VAT No. ..... No Tax Code/VAT No. ☐

Role: ◦ Joint controller ◦ Processor ◦ Representative

Section C: Summary of the incident that caused the data breach

1. When did the breach take place?

- ○ On _____
- ○ From _____ (the breach is still ongoing)
- ○ From _____ to _____
- ○ Has not yet been determined

Further information about the dates when the breach occurred

[6] This also includes processors pursuant to Art. 28, Para. 4

[7] In the case of a natural person, please enter the full name.

2. **When did the Data Controller become aware of the breach?**
   Date: Time:

3. **How did the Data Controller become aware of the breach?**
   o The Data Controller was informed by the Data Processor
   o Other[8]

4. **If more than 72 hours have passed between detection and Notification, what were the reasons for this delay?[9]**

5. **Brief description of the breach**

6. **Nature of the breach**
   ☐ a) Loss of confidentiality[10]
   ☐ b) Loss of integrity[11]
   ☐ c) Loss of availability[12]

7. **Cause of the data breach**
   ☐ Internal intentional action
   ☐ Internal accidental action
   ☐ External intentional action
   ☐ External accidental action
   ☐ Unknown
   ☐ Other (please specify)

8. **Categories of personal data affected by the breach**
   ▫ Personal identifiers (forename, surname, gender, date of birth, place of birth, tax code, or other)
   ▫ Contact details (postal or e-mail address, landline or mobile telephone number)

[8] For example: Reported by a data subject, informed by a third party, etc.

[9] Only complete for late notifications.

[10] Accidental or unauthorised disclosure of, or access to, personal data.

[11] Accidental or unauthorised alteration of personal data.

[12] Accidental or unauthorised loss of access to, or destruction of, personal data.

- ▫ Access and identifying data (username, password, customer ID, or other)
- ▫ Payment data (account number, credit card details, or other)
- ▫ Data relating to the provision of an electronic communications service (traffic data, data relating to internet browsing, or other)
- ▫ Data relating to criminal convictions and offences or related security or protection measures. Profiling data
- ▫ Data relating to ID documents (ID card, passport, driving license, national health card, or other)
- ▫ Location data
- ▫ Data revealing racial or ethnic origin
- ▫ Data revealing political opinions
- ▫ Data revealing religious or philosophical beliefs
- ▫ Data revealing trade union membership
- ▫ Data concerning sex life or sexual orientation
- ▫ Data concerning health
- ▫ Genetic data
- ▫ Biometric data
- ▫ Not yet known
- ▫ Other

9. **Enter the number (even approximate) of personal data records affected by the breach[13]**

   o No. _____

   o Approximate No. _____

   o Not (yet) known

10. **Categories of data subjects affected by the breach**
    - ▫ Employees/Consultants
    - ▫ Users/Contractors/Subscribers/Clients (current or prospective), Associates, Partners, Adherents, Supporters, Advocates
    - ▫ Corporate officers
    - ▫ Beneficiaries or clients
    - ▫ Patients
    - ▫ Children
    - ▫ Vulnerable groups (e.g. victims of violence or abuse, refugees, asylum seekers)
    - ▫ Not yet known
    - ▫ Other (please specify)

    - ▫ Further details about the categories of data subjects affected

11. **Number (even approximate) of data subjects affected by the breach**

    o _____ data subjects

    o Approximately _____ data subjects

    o Not (yet) known

[13] For example, the number of reports, number of database records, number of recorded transactions.

Section D: Detailed information on the data breach

1. **Description of the security incident which caused the breach**[14]

2. **Description of the categories of personal data affected by the breach**[15]

3. **Description of the IT systems and infrastructure involved in the incident, including their location**

4. **Technical and organisational protection measures implemented to protect the security of the data, IT systems and infrastructures involved**[16]

Section E: Potential consequences and severity of the breach

1.Possible impact on data subjects as a result of the breach

[14] Following on from Point 5, 6 and 7 of Section C.
[15] Following on from Point 8 of Section C
[16] Describe the measures in place when the breach occurred

a) In the event of a loss of confidentiality:[17]

- ▫ The data was disclosed outside the terms of the privacy policy or applicable law
- ▫ The data can be correlated, without unreasonable effort, to other information concerning the data subjects
- ▫ The data can be used for purposes other than those envisaged or in an unlawful way
- ▫ Other (please specify)

b) In the event of a loss of integrity:[18]

- ☐ The data has been modified and rendered inconsistent.
- ☐ The data has been modified but remains consistent
- ☐ Other (please specify)

c) In the event of a loss of availability:[19]

- ☐ Lack of access to services
- ☐ Malfunction and difficulty in using services
- ☐ Other (please specify)

Further considerations about the potential consequences

2.Potential negative impact on the data subjects

- ▫ Loss of control over their personal data
- ▫ Limitation of rights
- ▫ Discrimination
- ▫ Identity theft
- ▫ Fraud
- ▫ Financial loss
- ▫ Unauthorised reversal of pseudonymisation
- ▫ Damage to reputation
- ▫ Loss of confidentiality of personal data protected by professional secrecy
- ▫ Their information has become available to unauthorised third parties
- ▫ Any other significant financial or social disadvantage (please specify)

[17] Only to be completed if you have selected option a) of Point 6, Section C

[18] Only to be completed if you have selected option b) of Point 6, Section C

[19] Only to be completed if you have selected option c) of Point 6, Section C

3.Estimate of the seriousness of the data breach

o Negligible

o Low

o Medium

o Other

Please give details

Section F: Measures taken as a result of the breach

1. **Technical and organisational measures applied (or proposed to be taken[20]) to fix the breach and limit any adverse effects on the data subjects**

2. **Technical and organisational measures applied (or proposed to be taken) to prevent a recurrence of a similar breach**

Section G: Communication to Data Subjects

1. **Have data subjects affected by the breach been informed?**

o Yes, they were informed on _____

o No, but they will be informed

on _____
on a date yet to be determined

o No, investigations are still ongoing[21]

o No, and they will not be informed because:

a) the data controller believes that the personal data breach does not pose a high risk to the rights and freedoms of natural persons.
Explain the reasons why:

[20] In the description distinguish between actions which have already been taken and those in the process of being taken
[21] If this option is selected, the data controller must submit a follow-up to this notification

b) the data controller has implemented proportionate technical and organisational protection measures, and those measures have been applied to the personal data affected by the data breach, in particular measures that render the personal data unintelligible to any person who is not unauthorised to access it.

Describe the measures applied:

c) the data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

Describe the measures taken:

d) such communication would involve disproportionate effort. Describe the method by which the data subjects affected by the breach have been informed (public announcement or similar means).

2. **Number of data subjects who have been informed about the breach[22]**

_____ data subjects

3. **What information have the Data Subjects been told?**

4. **What means of communication have been used to inform the Data Subjects?**

- ☐ SMS
- ☐ Post
- ☐ E-mail
- ☐ Other (please specify)

[22] Only to be completed if one of the first two options in Point 1 have been selected.

Section H - Other information

1. **Does the breach affect data subjects in other European Economic Area countries[23]?**
   - o YES (indicate which):
   - o NO

2. **Does the breach affect data subjects in countries not belonging to the European Economic Area?**
   - o YES (indicate which):
   - o NO

3. **Have other supervisory authorities been notified about the breach[24]?**
   - o YES (indicate which):
   - o NO

4. **Have other supervisory or monitoring organisation been notified about the breach, by virtue of other legislative provisions[25]?**
   - o YES (indicate which):
   - o NO

5. **Have judicial authorities or the police been informed?**
   - o YES
   - o NO

*** *** ***

The following documents are attached:

1) Assessment of the risk to the rights and freedoms of natural persons.

2) Data Breach Register.

Rome, on [*insert date*]

Data Controller

Good Shepherd International Foundation Onlus

_____

[23] All Member States of the European Union are part of the European Economic Area, as well as Iceland, Liechtenstein and Norway

[24] Supervisory authority as defined pursuant to Art. 51 of Regulation (EU) 2016/679

[25] For example: Regulation (EU) N° 910/2014 (eIDAS), Leg. Decree No. 65/2018 which duly implements the Directive (EU) 2016/1148 (NIS)

INFORMATION TECHNOLOGY

TABLE OF CONTENTS

1. GSIF Digital Archive
1.1 SharePoint
1.2 File naming
2. GSIF ERP
2.1 Finance and Accounting Section
2.2 Project and Program Section
3. PROLEA
4. Microsoft Teams
5. Some recommendations on e-mail use

1. GSIF DIGITAL ARCHIVE

A digital archive is similar in purpose to a physical archive, but the historical documents and objects that provide evidence of the past have been digitized (often by scanning or photography, unless a document was created digitally in the first place) and made available online. Digital archives are usually created with a goal of preserving historical objects and making them available to researchers.

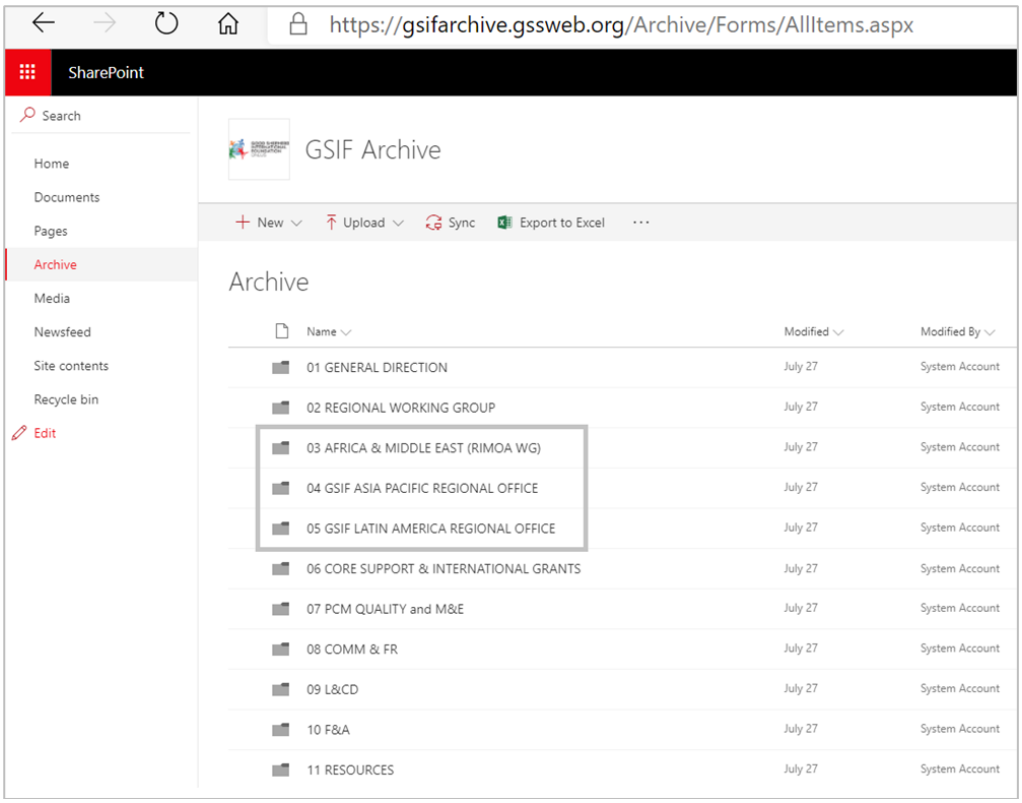
In our organization **Digital Archive** is the space where all GSIF staff should store all documents relevant for GSIF's work. In order to access the Digital Archive users can access SharePoint, click on the right toolbar on Digital Archive (or if they need a project, click on Projects Folders). On SharePoint users can upload existing documents from the hard drive, create and save new documents or modify an existing document. For all these options, goon the top left bar and click on "Documents". The menu will give options for all the available functions: upload, new item, edit, etc. To keep browsing SharePoint, hit back on "Browse". To find documents in the Digital Archive you can use the internal search engine on the top right.

1.1 SharePoint

SharePoint is a document management and collaboration tool developed by Microsoft. It's basically an intranet and content management system that is used for internal purposes to assist with bringing an organization together. SharePoint is a highly customizable application, one that is designed to accommodate your changing needs. GSIF is also using this system to create and maintain the digital archive. We have a **Central Location for All our Important Documents**, the important documents are all saved under one common location, so there is no loss of data or difficulty finding the right information at any time.

The SharePoint database is accessible from the HQ in Rome via cable and from everywhere in the world via Internet at **https://gsifarchive.gssweb.org/Archive/Forms/AllItems.aspx**.

Access to some sensitive sections of the database is restricted. Each GSIF staff members has a username and password to login. Usernames and passwords are created and modified only by the IT administrator.



Since SharePoint offers a number of different functionalities, it's used by a wide range of businesses and organizations of all sizes.

Some of the uses of SharePoint:

- Collaboration
- Document Management
- Document Sharing
- Intranet Services

All GSIF staff and partners are invited to save/upload in the relevant folders of the SharePoint Digital Archive the following documents: projects, applications to national and international funding agencies, all documents related to the grants received, general presentations of the Rome and regional MDOs, general presentations of the programs, information on the GSIF staff, pictures related to the projects sites or to the Good Shepherd programs.
The SharePoint can set up document libraries to allow for easy document sharing, setting up group calendars to track projects, tasks, meetings and events or creating custom workflows that simplify your specific processes, The SharePoint homepage has also a section dedicated to share external resources. All users are invited to post links on interesting documents, websites and any other relevant information for GSIF's work.
GSIF staff in Rome and in the regional offices can still store working documents on their own computer "C" drive (hard disk), however, everybody is invited to save a copy of those documents (at least the final version) in SharePoint.
All documents saved in SharePoint are retrievable by our IT administrator and there is a regular backup done at central level. This way even if your computer crashes, the digital archive is safe with all your documents.

The SharePoint database is accessible from any computer, tablet or smartphone connected to the internet. Open your favorite web browser window and type the URL: **https://gsifarchive.gssweb.org/Archive/Forms/AllItems.aspx**
Access to some sensitive sections of the database is restricted. Each MDO staff members in Rome and in the local offices has a username and password to login. From the login page, use the same username and password you would use for your @gssweb.org email address.

1.2 File naming

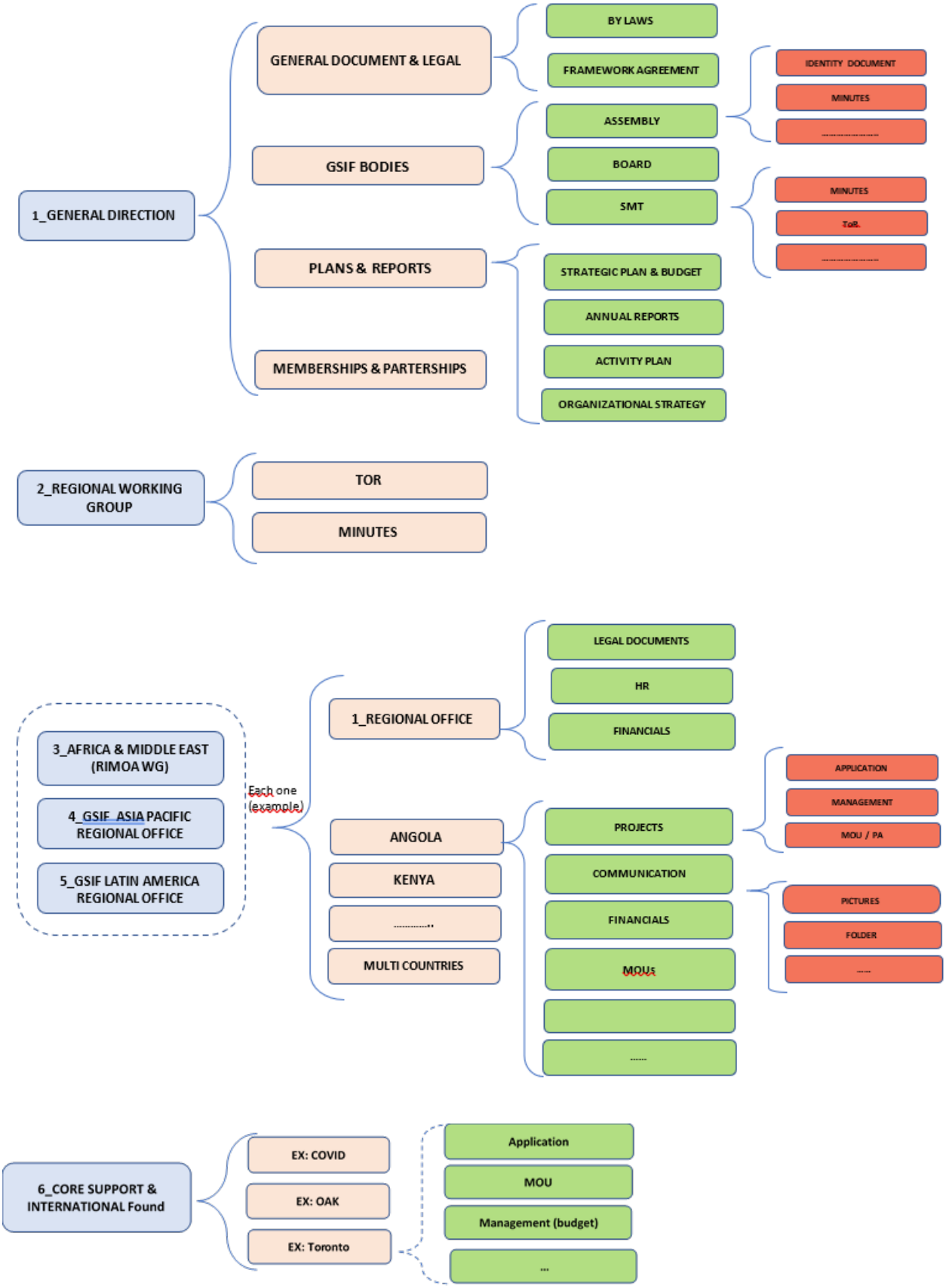
Recommendations for file naming:

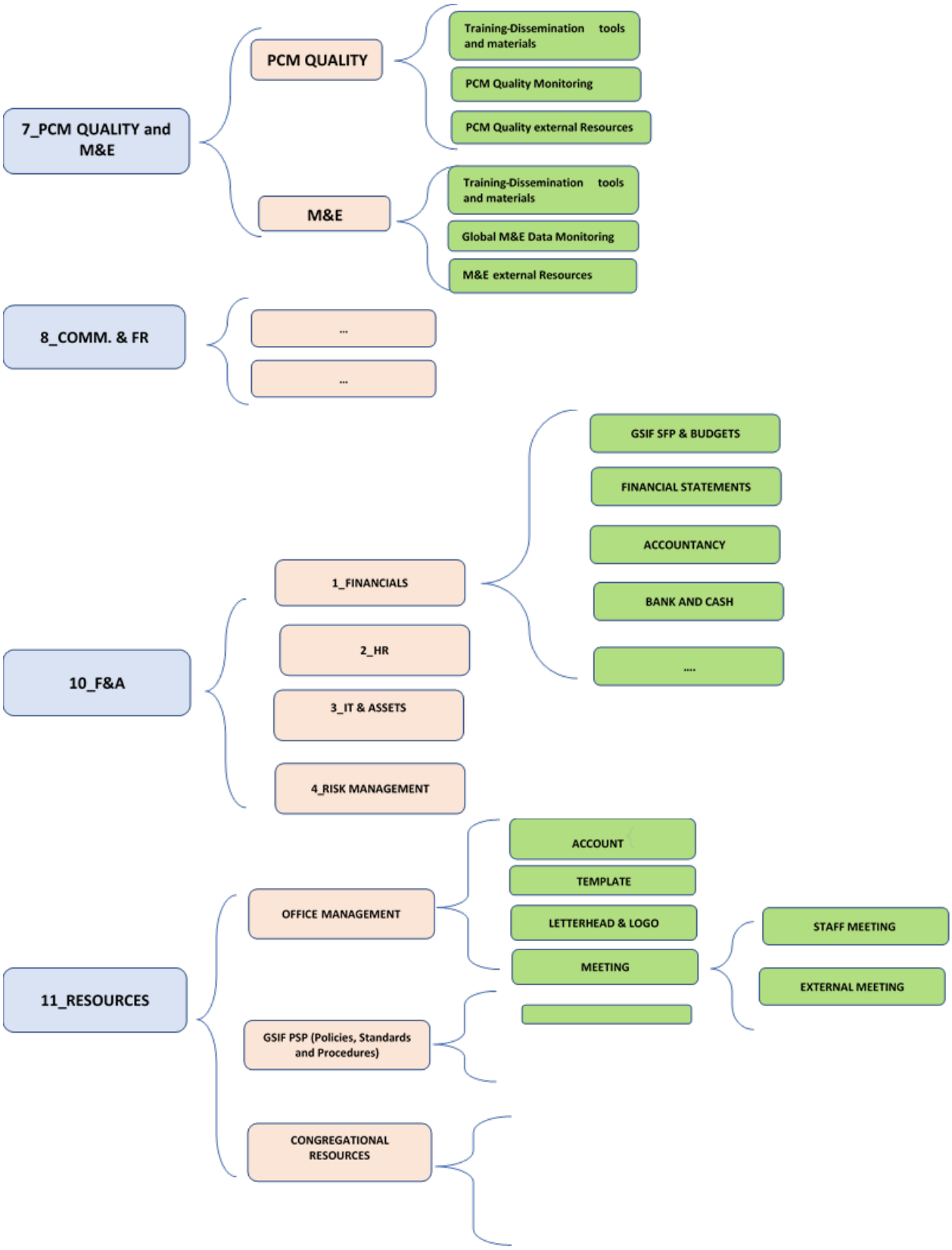
ITEM	RULE	EXAMPLE
COUNTRY	Indicate acronym of the country the document refers to. *Use the country codes of ERP*	DRC = Democratic Republic of Congo LEB = Lebanon ANG = Angola IND = India BOL = Bolivia MEX = Mexico
SUBJECT/ TYPE OF DOCUMENT	File names should be short but descriptive. Can include key word of the project title, acronym of the funding agency for applications or name of the city where a project is developed.	Kikolo School_CEI Childreen Home_OAK Migration_HF Casas Mujeres Emprendedoras Emergency COVID *Use abbreviations like:* Economic Justice = EJ Human Rights = HR Human Trafficking = AHT Capacity Building = CB *Use acronyms for Funding agencies:* Misean Cara = MC Harris Fraser = HF The One Body One Spirit Movement = OBOS
	or qualify the nature of the document.	report authorization letter presentation *Use abbreviations like:* application = app budget = bdgt
DATE	Indicate the date of creation of the document – European dating system GG MM AA	Kikolo School_CEI_140820

Examples:
ANG_Kikolo School_140820
DRC_Report GIZ_131120

1.3 Map of the folders

The Digital Archive is articulated in the following folders:




7_PCM QUALITY and M&E
PCM QUALITY
Training-Dissemination tools and materials
PCM Quality Monitoring
PCM Quality external Resources
M&E
Training-Dissemination tools and materials
Global M&E Data Monitoring
M&E external Resources
8_COMM. & FR
...
...
10_F&A
1_FINANCIALS
GSIF SFP & BUDGETS
FINANCIAL STATEMENTS
ACCOUNTANCY
BANK AND CASH
....
2_HR
3_IT & ASSETS
4_RISK MANAGEMENT
11_RESOURCES
OFFICE MANAGEMENT
ACCOUNT
TEMPLATE
LETTERHEAD & LOGO
MEETING
STAFF MEETING
EXTERNAL MEETING
GSIF PSP (Policies, Standards and Procedures)
CONGREGATIONAL RESOURCES

2. GSIF ERP

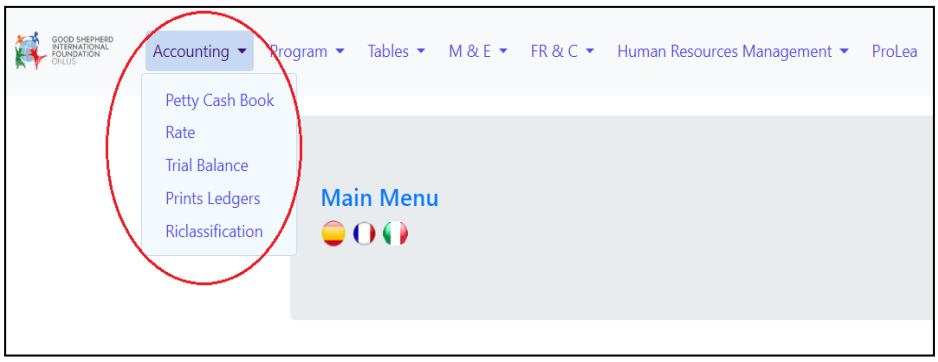
GSIF ERP (Enterprise Resource Planning) is an **integrated management tool** that GSIF uses to collect, store, manage, and interpret data with regard to different sets of activities.
It aims to enhance the organizational efficiency and effectiveness with regard to the following areas:

- Finance and Accounting;
- Project/Program Management;
- Project/Program Monitoring and Evaluation;
- CRM (Customer Management Relations);
- E-learning resources and processes;
- Human Resources Management;
- Program Strategic Financial Plans;
- Data consistency: a common database aiming to supports all the applications.

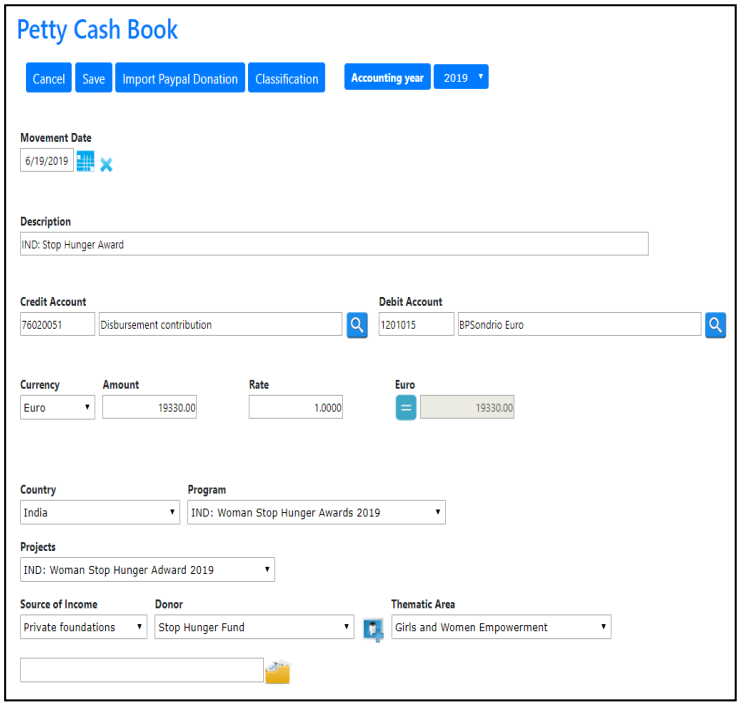
It is a multi-language (English, Spanish, French and Italian) on-line platform accessible from anywhere you have an internet connection. The link: https://gsif.gssweb.org/

2.1 Finance and Accounting Section

Finance and Accounting Section is managed by the **GSIF F&A Desk**. In this section, we keep **the Official Accounting System** and we elaborate the GSIF **Annual Financial Statement**.



Every record is classified by a set of variables (such as Country, Program, Project, Donor, Thematic Area) in order to allow the F&A Department to analyze the financial data and organize them for different purposes.



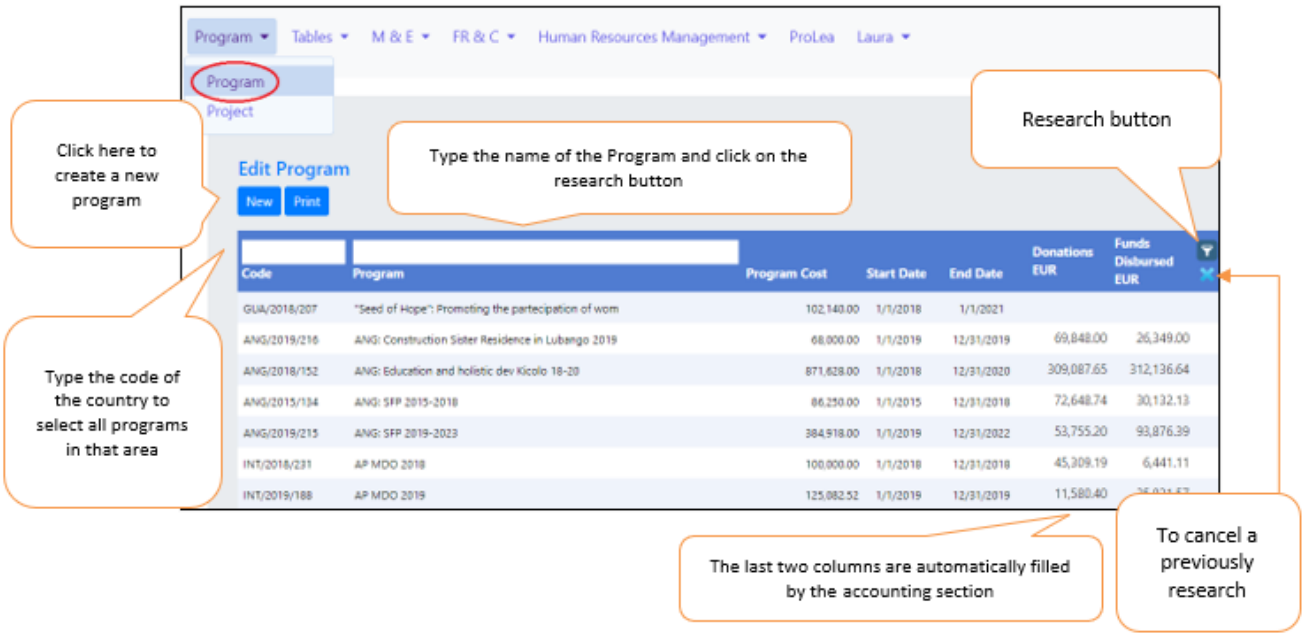
2.2 Project and Program Section

The **Program Section** is managed by the **GSIF Program Department**. In this section, we keep the **Database of the Projects** (grants and applications) **and the Programs to which they refer.**

This section is fundamental for the management of the Projects and Program. The Program Managers are supposed to fill in and update constantly this section by selecting a specific program, inserting the requested data, and periodically update the logbook.

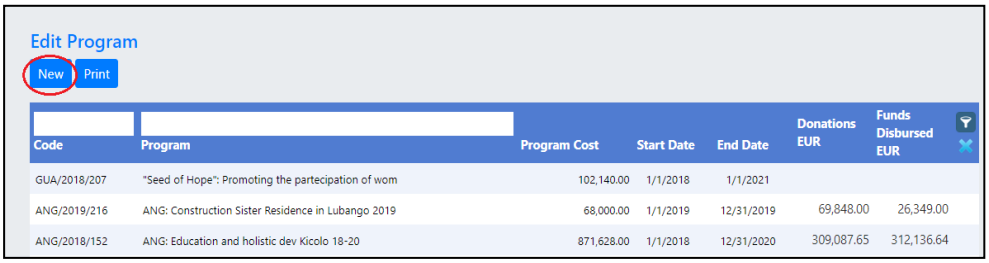
Program List and Form

A Program is a set of projects and interventions over several years whose objective is a long- term response to the needs identified by your organization. It stems directly from the strategic plan. To manage the programs archive, open the program section from the main menu. You can show the list of the programs, research and manage it.



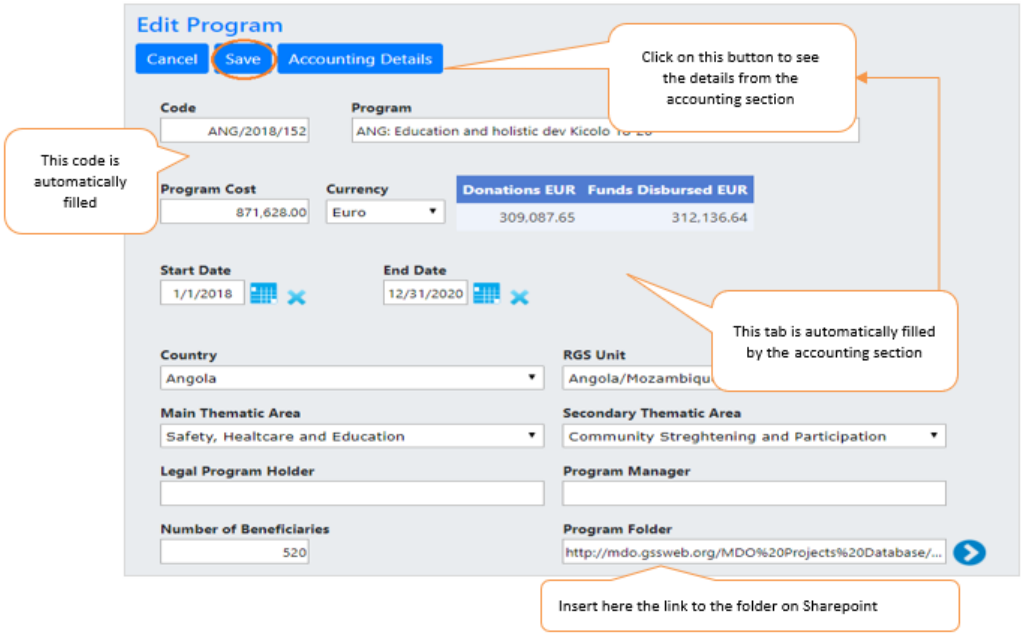
How to create or modify a Program?

To create a new program**:** from the program's list click on "New" and fill up the form.



To modify a program: select a Program from the list. Click on “Edit” and it will open the analytical description/form of the Program.

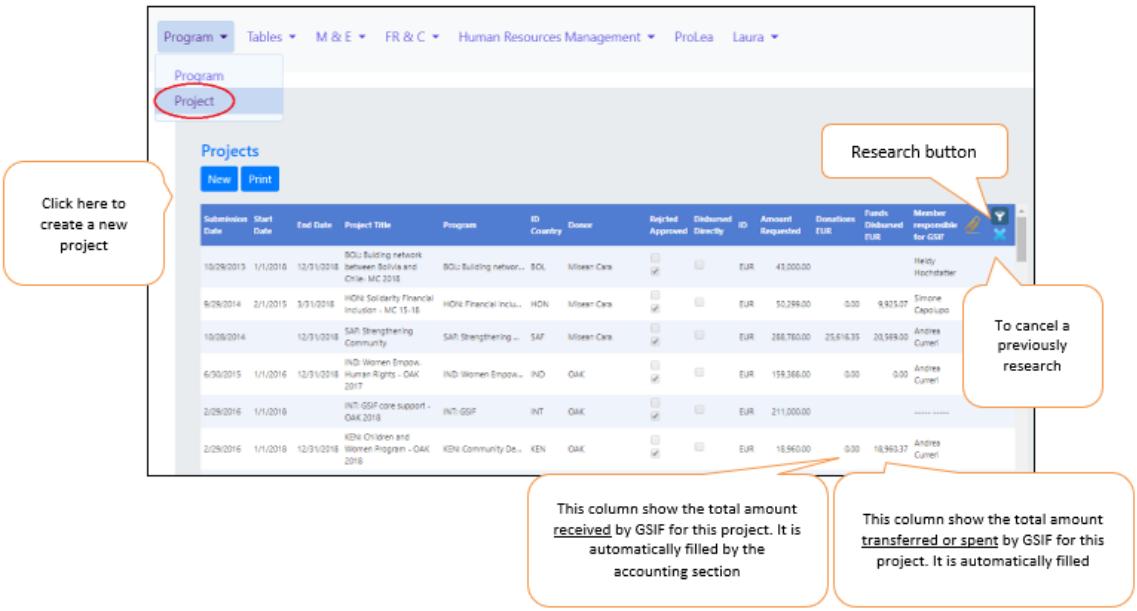
This below is the program form. Edit or update the information regarding the Program.



Project List and Form

A Project is a set of activities and actions properly coordinated and with a high degree of autonomy which contributes to the achievement one or more objectives of the Program.

To manage the project archive open the project section from the main menu. You can show the list of the project, research and manage it.

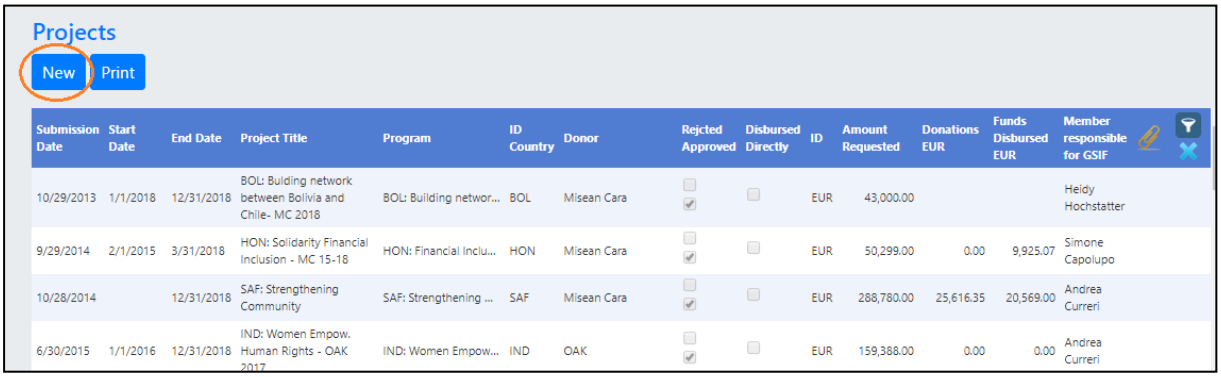


How to search for a Project?

Click on the research button and it will open the research form. Here you can choose a period, type a part of the project name or select some other information about the project you are looking for. Click on "Filter" to start the research or "Cancel" to come back at the project list.

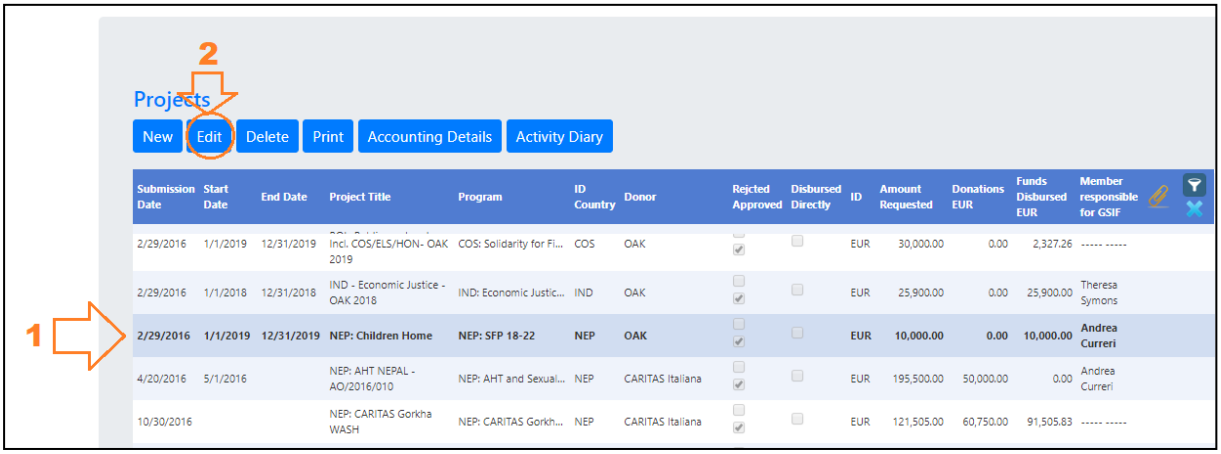
How to create or modify a Project?

To create a new project**:** from the list click on "New" and fill up the form.



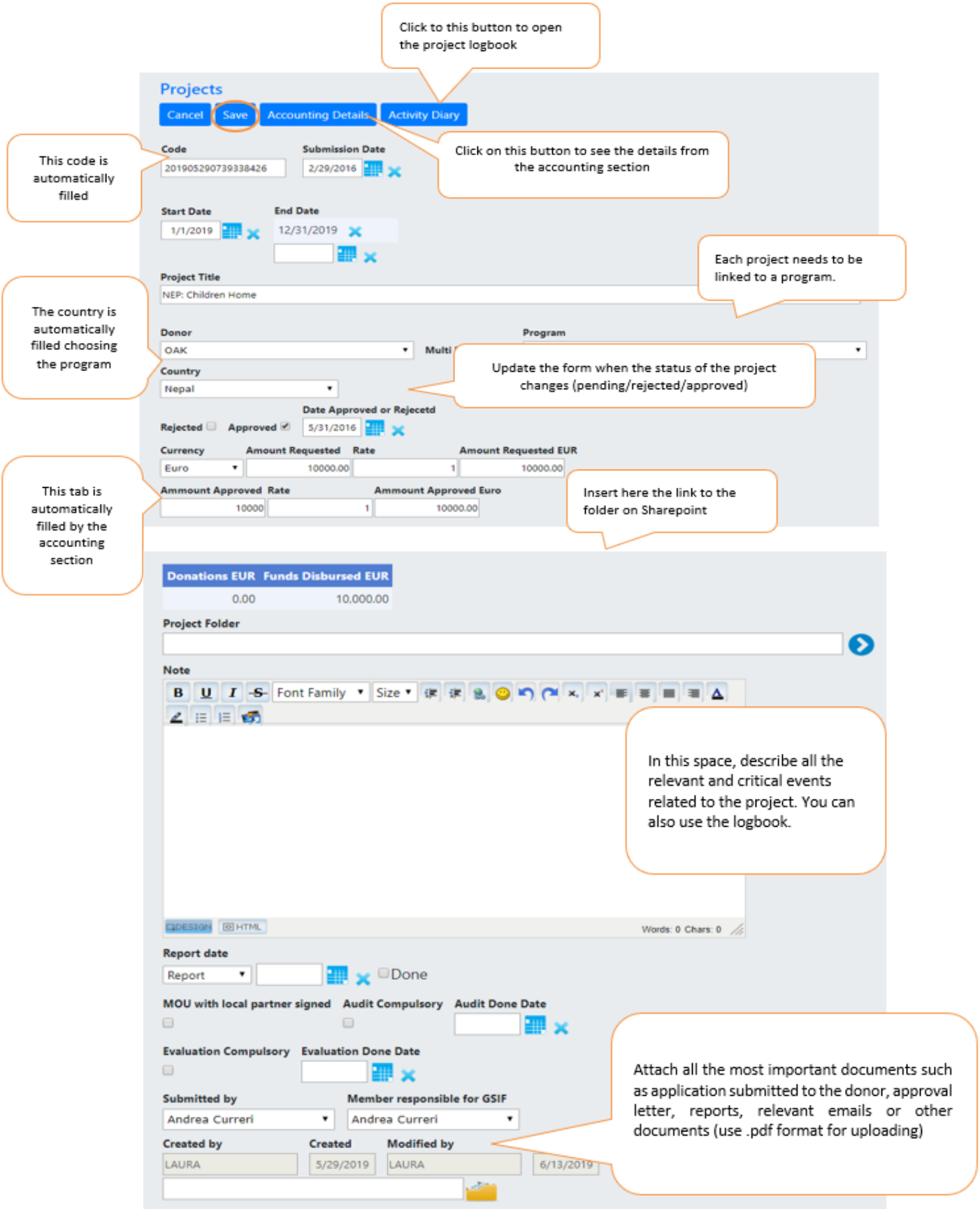
Submission Date	Start Date	End Date	Project Title	Program	ID Country	Donor	Rejcted Approved	Disbursed Directly	ID	Amount Requested	Donations EUR	Funds Disbursed EUR	Member responsible for GSIF
10/29/2013	1/1/2018	12/31/2018	BOL: Building network between Bolivia and Chile- MC 2018	BOL: Building networ...	BOL	Misean Cara			EUR	43,000.00			Heidy Hochstatter
9/29/2014	2/1/2015	3/31/2018	HON: Solidarity Financial Inclusion - MC 15-18	HON: Financial Inclu...	HON	Misean Cara			EUR	50,299.00	0.00	9,925.07	Simone Capolupo
10/28/2014		12/31/2018	SAF: Strengthening Community	SAF: Strengthening ...	SAF	Misean Cara			EUR	288,780.00	25,616.35	20,569.00	Andrea Curreri
6/30/2015	1/1/2016	12/31/2018	IND: Women Empow. Human Rights - OAK 2017	IND: Women Empow...	IND	OAK			EUR	159,388.00	0.00	0.00	Andrea Curreri

To modify a project: select a Project from the list. Click on "Edit" and it will open the analytical description/form of the Project.



Submission Date	Start Date	End Date	Project Title	Program	ID Country	Donor	Rejcted Approved	Disbursed Directly	ID	Amount Requested	Donations EUR	Funds Disbursed EUR	Member responsible for GSIF
2/29/2016	1/1/2019	12/31/2019	Incl. COS/ELS/HON- OAK 2019	COS: Solidarity for Fi...	COS	OAK			EUR	30,000.00	0.00	2,327.26	----- -----
2/29/2016	1/1/2018	12/31/2018	IND - Economic Justice - OAK 2018	IND: Economic Justic...	IND	OAK			EUR	25,900.00	0.00	25,900.00	Theresa Symons
2/29/2016	**1/1/2019**	**12/31/2019**	**NEP: Children Home**	**NEP: SFP 18-22**	**NEP**	**OAK**			**EUR**	**10,000.00**	**0.00**	**10,000.00**	**Andrea Curreri**
4/20/2016	5/1/2016		NEP: AHT NEPAL - AO/2016/010	NEP: AHT and Sexual...	NEP	CARITAS Italiana			EUR	195,500.00	50,000.00	0.00	Andrea Curreri
10/30/2016			NEP: CARITAS Gorkha WASH	NEP: CARITAS Gorkh...	NEP	CARITAS Italiana			EUR	121,505.00	60,750.00	91,505.83	----- -----

To the next page there is the project form. Edit or update the information regarding the Project.


Click to this button to open the project logbook
Projects
Cancel
Save
Accounting Details
Activity Diary
Click on this button to see the details from the accounting section
This code is automatically filled
Code
20190529073933842 6
Submission Date
2/29/2016
Start Date
1/1/2019
End Date
12/31/2019
Each project needs to be linked to a program.
Project Title
NEP: Children Home
The country is automatically filled choosing the program
Donor
OAK
Program
Country
Nepal
Update the form when the status of the project changes (pending/rejected/approved)
Date Approved or Rejecetd
Rejected
Approved
5/31/2016
Currency
Amount Requested
Rate
Amount Requested EUR
Euro
10000.00
1
10000.00
This tab is automatically filled by the accounting section
Ammount Approved
Rate
Ammount Approved Euro
10000
1
10000.00
Insert here the link to the folder on Sharepoint
Donations EUR
Funds Disbursed EUR
0.00
10,000.00
Project Folder
Note
Font Family
Size
DESIGN
HTML
Words: 0 Chars: 0
In this space, describe all the relevant and critical events related to the project. You can also use the logbook.
Report date
Report
Done
MOU with local partner signed
Audit Compulsory
Audit Done Date
Evaluation Compulsory
Evaluation Done Date
Submitted by
Andrea Curreri
Member responsible for GSIF
Andrea Curreri
Created by
LAURA
Created
5/29/2019
Modified by
LAURA
6/13/2019
Attach all the most important documents such as application submitted to the donor, approval letter, reports, relevant emails or other documents (use .pdf format for uploading)

2.2.1 How to see the details from the accounting section?

Select a Project from the list. Click on “Accounting Details” and it will open the analytical form of the accounting section.

Submission Date	Start Date	End Date	Project Title	Program	ID Country	Donor	Rejcted Approved	Disbursed Directly	ID	Amount Requested	Donations EUR	Funds Disbursed EUR	Member responsible for GSIF
7/13/2017	1/1/2018		ANG: Education and holistic dev Kicolo - HF	ANG: Education and ...	ANG	Harris Fraser			USD	320,000.00	283,134.00	197,478.64	Andrea Curreri
1/1/2018			Education and prevetion of child labour in South Quito	Education and preve...	ECU	Harris Fraser			EUR	180,000.00			Heidy Hochstatter
6/7/2018	1/1/2019	12/31/2019	MAD: Building Holistic Development for Morondava -HF	MAD: Building Holist...	MAD	Harris Fraser			USD	57,540.62	51,682.98	2,667.60	----- -----
7/21/2018	1/1/2019		DRC: Children not miners - BP Kolwezi 2018-2022 -HF	DRC: Children not mi...	RDC	Harris Fraser			USD	120,000.00	35,478.90	0.00	Simone Capolupo
8/17/2018	11/1/2018	10/31/2021	BFA: Protecting and empowering girls, wom. and chldren - HF 19-22	BFA: Protecting and ...	BFA	Harris Fraser			USD	77,700.00	28,437.01	0.00	----- -----
8/17/2018	**1/1/2019**	**12/31/2019**	**INT: Capability Development of GSS in Africa -HF**	**INT: Capability Dev...**	**INT**	**Harris Fraser**			**USD**	**260,320.00**	**116,766.00**	**13,918.76**	**Giovanna Reda**
2/18/2019	8/1/2019	7/31/2020	BFA: Construction - HF 2019	BFA: Protecting and ...	BFA	Harris Fraser			USD	112,475.75			Giovanna Reda

This accounting list is automatically filled by the accounting section.

Movement Date	Description	Donations EUR	Funds Disbursed EUR
2/18/2019	INT: Capability Development of GSS in Africa- HF- rimborso spese Calvin Mackay	0.00	83.76
4/1/2019	RAPTIM EC 397 marzo - Mathilde Roma	0.00	360.00
4/26/2019	INT: Cap Dev Africa - Donazione Harris Fraser 2019	116,766.00	0.00
5/3/2019	Visto DRC Zelna	0.00	115.00
5/13/2019	INT: Cap Dev Africa - Workshop Kolwezi	0.00	13,360.00

The **Tables Section** is managed by the **ORP Administrators**. In this section, we keep the various sets of data related to the OPR’s users, the chart of account, the exchange rate management, etc.

3. ProLea

Online learning is the newest and most popular form of distance education today. Within the past decade it has had a major impact on postsecondary education and the trend is only increasing. In this platform we will explore what the experience of online learning is like for students and how it has changed the role of the instructor.

Our platform offer's functionality which allows instructors to deliver course content, enable communications, and conduct evaluations. The most common tools offered by platform include:

Schedule For posting and viewing deadlines, events, etc.
Announcements For posting current information to all students.
Syllabus For creating and posting the course syllabus.
Modules For publishing and viewing course content in sections.
Assignments For posting, submitting, and grading student work.
Discussion Board For asynchronous discussions, group work, and collaboration.
Private Messages For private communication between students and/or the instructor.
Chat For real-time, synchronous conversation in written form.
Tests & Quizzes For authoring and administering exams, quizzes, surveys, etc.
Gradebook For posting and managing student grades.

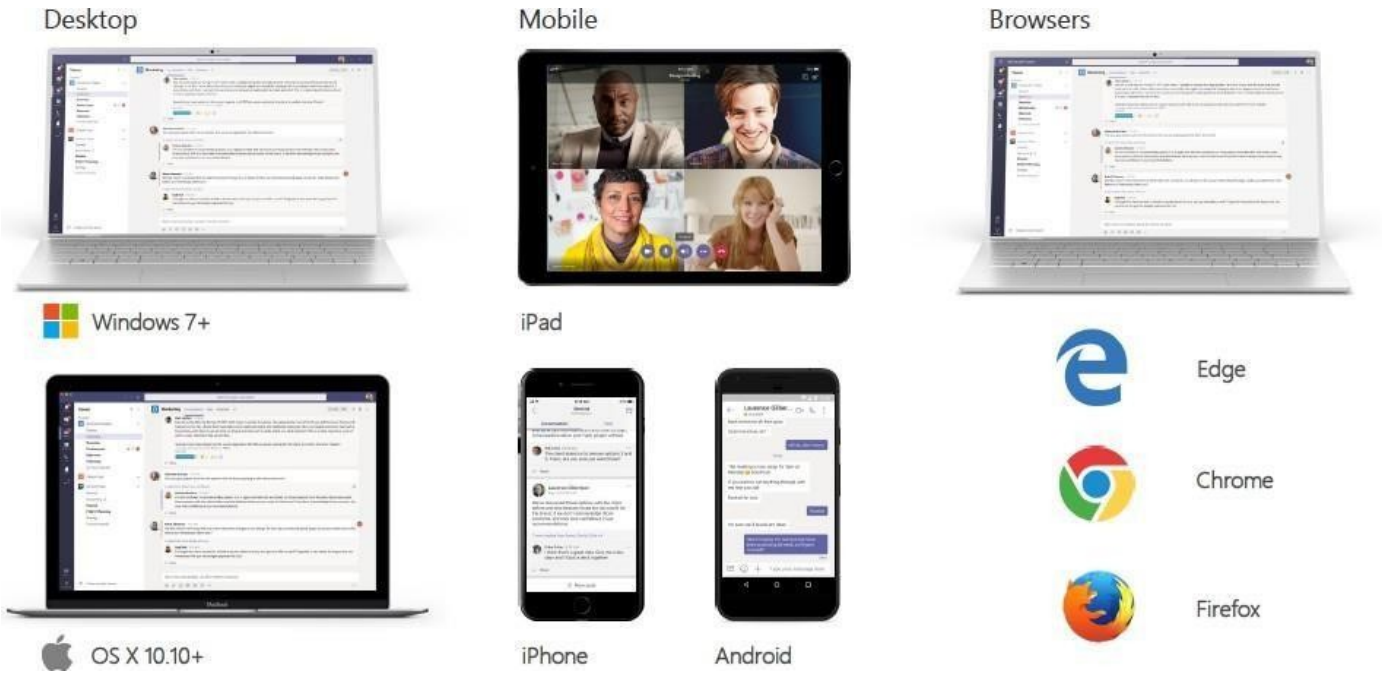
4. Microsoft Teams

Microsoft Teams is a persistent chat-based collaboration platform complete with document sharing, online meetings, and many more extremely useful features for communications. Having an excellent feature is a key to everyone to make creative decisions and communicate with one another.

What MS Teams can do?

- Communicate with your people in chat message, voice, video conference, and screensharing;
- MS Teams supports a large group of users in a voice/video conference meeting. It is good for virtual lecture, project discussion, andmeetings;
- Exchange information with file sharing and channels;
- Introduction to Teams (duration: 2 minutes): https://support.office.com/en-us/article/video-welcome-to-microsoft-teams-b98d533f-118e-4bae-bf44-3df2470c2b12?ui=en-US&rs=en- US&ad=US
- Browser: Internet Explorer/Google Chrome (** Safari browser is not supported), desktop clients, and mobile apps (Google Play/Apple AppStore.

Supporting platforms



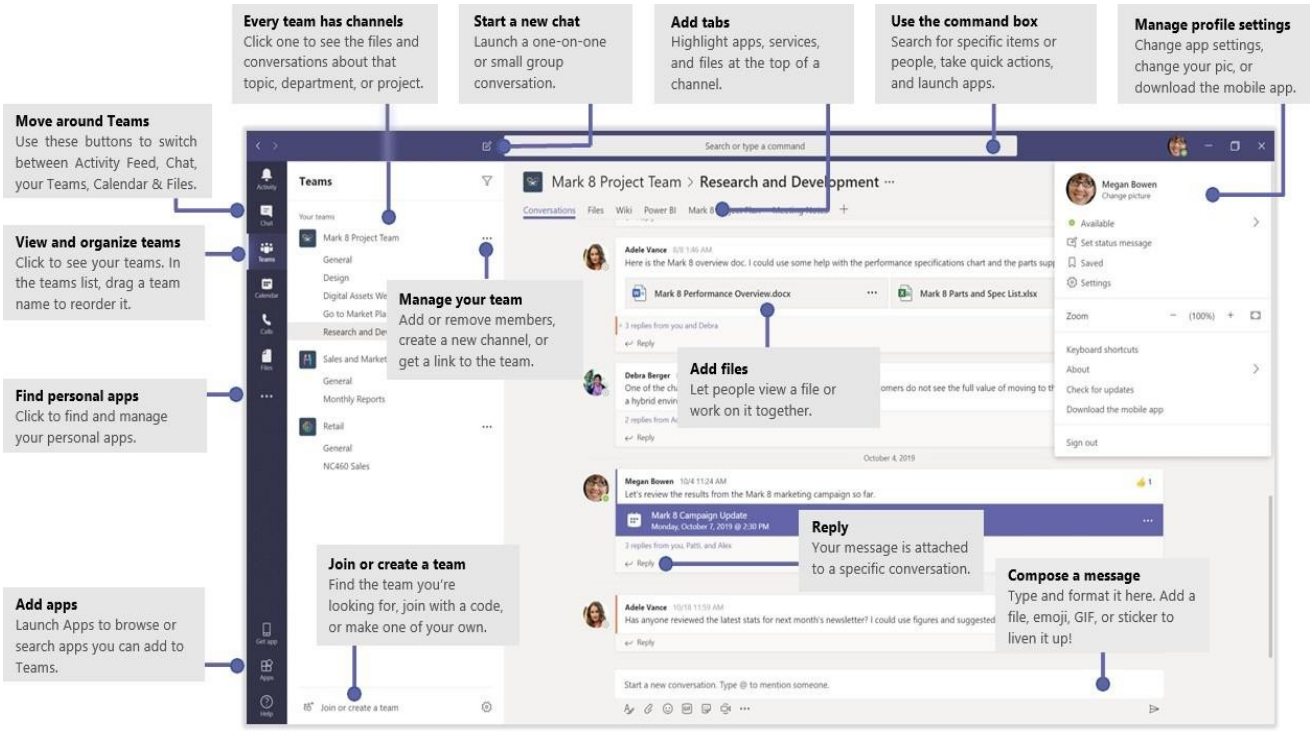
Login to MS Teams

Web browser	**Teams client**	**Mobile App**
Login to https://teams.microsoft.com/	Click on Teams icon on the desktop	Click on **Teams App** on mobile or Pc
Account & Password:	**<your NETID>@connect.polyu.hk** and **Connect password**	

4.1 Basic features on MS Teams

Microsoft Teams provides chat-based workspace where team members can share ideas, documents and calendars as well as hold discussion and make video calls, etc. Teachers can create collaborative classrooms, communicate with a large group of students in chat, voice, video conference, sharescreen as well as exchange information with file sharing and channels.

- Induction to MS Teams features - https://support.office.com/en-us/article/video-what-is- microsoft-teams-422bf3aa-9ae8-46f1-83a2-e65720e1a34d?ui=en-US&rs=en-US&ad=US
- Best features in MS Teams:https://www.youtube.com/watch?v=_Cw9uXfgTLQ



4.2 Chat with members

In Chat, you could start a discussion with all members in the group or privately to a specific person/member. Group members/students will receive Chat messages in both Teams client and Connect email account. It is a useful and effective feature to communicate with a group of people.

Video on Chat (duration: 1:30 minute): https://support.office.com/en-us/article/video-start-chats- and- make-calls-a864b052-5e4b-4ccf-b046-2e26f40e21b5?ui=en-US&rs=en-US&ad=US

Video on get attention with @mention (duration: 0:41 minute): https://support.office.com/en- us/article/get-attention-with-mentions-b2ffb135-7069-4880-84ee-5b27f402418b

4.2.1 View a chat

- **Chat** and select a one-on-one or group chat from the chat list.

4.2.2 Start a chat

- Select **New chat** .
- Type the name of the person or people you want to contact.
- Select the down arrow to add a name to your chat group.

4.2.3 Get one person's attention

- Type a message in a reply or start a new conversation.
- Type @ and the person's name.
- Select the person's name you want to mention.
- Finish your message and select **Send**.

4.2.4 Get an entire team or channel's attention

- Type a message in a reply or start a new conversation.

- Type **@team** or **@channel**.
- Select the team or channel you want to mention.
- Finish your message and select **Send**.

4.2.5 Make video and audio calls from a chat

- Select **Video call** or **Audio call** to call someone directly from a chat.

4.2.6 Use Recent and Favorites

- On the left side of the app, you'll see your Recent conversations as well as your Favorites.
- Hover over a conversation, select the three dots, and then select **Favorite** to keep your chat in your Favorites list.

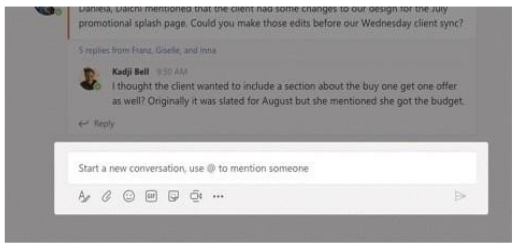
Sign in

In Windows, click **Start** > **Microsoft Teams**.
On Mac, go to the **Applications** folder and click **Microsoft Teams**.
On mobile, tap the **Teams** icon. Then sign in with your Office 365 username and password. (If you're using Teams free, sign in with that username and password.)

Start a conversation

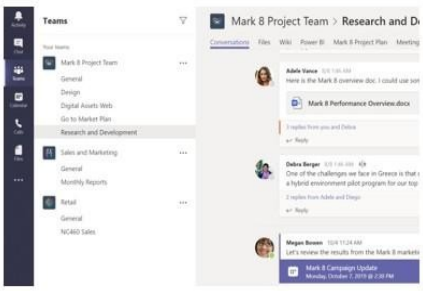
With the whole team... Click **Teams** , pick a team and channel, write your message, and click **Send** .

With a person or group... Click **New chat** , type the name of the person or group in the **To** field, write your message, and click **Send** .



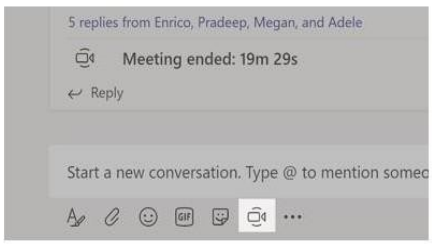
Pick a team and channel

A *team* is a collection of people, conversations, files, and tools—all in one place. A *channel* is a discussion in a team, dedicated to a department, project, or topic. Click **Teams** , select a team. Pick a channel to explore the **Conversations**, **Files**, and other tabs.



Start a meeting

Click **Meet now** under the area where you type a message to start a meeting in a channel. (If you click **Reply**, then **Meet now** , the meeting is based on that conversation.) Enter a name for the meeting, then start inviting people.



4.3 Scheduling and managing virtual meeting

- Video on Meet now (duration 2:11 minutes):
- https://support.office.com/en-us/article/videocreate-instant-meetings-with-meet-now-26e06837-853d-4df1-a729- 06bf700d4ecf?ui=en- US&rs=en- US&ad=US
- Video on schedule a meeting (duration 1:33 minutes):
- https://support.office.com/en- us/article/video-manage-meetings-ba44d0fd-da3c-4541-a3eb-a868f5e2b137?ui=en- US&rs=en- US&ad=US

4.3.1 Start a meeting

- To start a meeting, do one of the following:
- Select in a new conversation.
- Select in an existing conversation to keep all that conversation's context.
- In your video preview, enter a name for the meeting, and select **Meet now**.

- Select the names of the team members you want to invite to the meeting. You can also type a phone number, a good way to add people outside your organization that aren't using Teams.

4.3.2 Join a meeting

- Look for the meeting notification icon in a conversation to find a meeting.
- Select **Jump In** to participate in the meeting.

4.3.3 Share your screen

- Select the share screen icon to show your screen to the other people in the meeting.

4.3.4 Record your meeting

- Select more options icon to record the meeting. You'll be emailed when the video is ready so you can view, edit, and share with others.

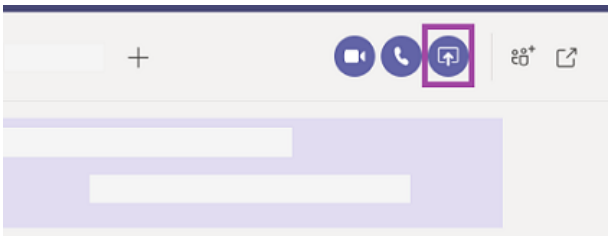
4.3.5 Sharing whiteboard

You can share a whiteboard to make it available to all participants in a Teams meeting. That same whiteboard is simultaneously available in the Whiteboard applications on Windows 10, iOS, and on the web.

- After joining a Teams meeting, click the **Share** icon in the share tray of thatmeeting.
- In the **Whiteboard** section, select **Microsoft Whiteboard**.

4.3.6 Sharing your screen

When you're chatting with one or more people in Teams, you can instantly share your screen.
Go to the chat controls in the upper-right corner and select **Share** .



- Choose a window to share that specific program and its content, or select **Desktop** to share everything on your screen.
- The other participants in the chat will receive a notification asking them to accept your screen share. Once they do, they'll be able to see your screen and continue the chat.
- When you're done sharing, go to your meeting controls and select **Stop sharing**.

Video on schedule a meeting (duration 1:33 minutes):
https://support.office.com/en-us/article/video-manage-meetings-ba44d0fd-da3c-4541-a3eb-a868f5e2b137?ui=en US&rs=en-US&ad=US

5. View meetings

- Select **Calendar** to view your appointments and meetings for the day or work week.
- These appointments stay synchronized with your Outlook calendar.
- Select a meeting invite to see what the meeting's about, who's attending, and to respond to the meeting.

5.1 Schedule a meeting (with external guests)

- Select **New meeting**.
- Type in a meeting title and enter a location. An online meeting is created by default.
- Choose a start and end time, and add details if needed.
- Enter names in the **Invite people** box to add them to the meeting.

Note: To invite someone outside your organization, type-in their email address and they'll get an invitation to join as a guest — even if they don't have Microsoft Teams.

- See everyone's availability in the **Attendees** list and, if needed, choose a suggested time or select **Scheduling assistant** to see more available times in a calendar view.
- Under **Select a channel to meet in**, select the drop-down arrow to manage your meeting's privacy settings:
- Select **None** to keep your meeting private.
- Select a channel to open the meeting to team members.

If your meeting gets posted in a channel, it'll appear under the **Posts** tab. Team members can set agendas, share files, or add comments.

Other resources

- Microsoft Teams training video: https://support.office.com/en-us/article/microsoft-teams-video-training-4f108e54-240b-4351-8084-b1089f0d21d7
- Other use tips and ideas: https://support.office.com/office-training-center/Teams-tips
- ITS Online training resources: https://www2.polyu.edu.hk/its/online- training/category.php?cat=MS%20Produ ct

Email Etiquette: CC and BCC Are Not Your Friends

(https://maurathomas.com/productivity/email-etiquette/)

Do you work at a company where everyone is copied on everything? My work has shown me that so much email a company generates is unnecessary, ineffective, and primarily unread. Many of these are sent as a cc or a bcc. The fact that these acronyms stand for "carbon copy" and "blind carbon copy" should give you an idea that their time has passed. Who even remembers what a "carbon copy" is?

I want to point out some of the reasons I have seen these used, and give you some ideas for improving your effectiveness with email.

Cc for FYI

Bad Idea: Sometimes a cc is used to "keep people in the loop." Perhaps you copy someone on an email because you want them to know what's going on. This is not the best way to keep your co-workers informed. First, your recipient has to read through the message to figure out why they got it. And then they may not glean from it what you intended them to know. What's more likely, if the message is not addressed to them, they probably didn't read it at all. Maybe they just deleted it, or perhaps they moved it to a reference folder, or they marked it as unread but kept it in their inbox. All of these are ineffective for the recipient, because they cause clutter, but also you have not met your objective by sending it to them in the first place. This is one of the most frequent causes of communication breakdown in an organization.

Better: If you want someone to know something you've put in an email, cut and paste the information and send it in a separate email directly to them. Then there is no chance for misinterpretation and a lower chance that it will be overlooked. Alternately, address them directly in the original message, near the top. For example, "Hi Jane – I'm writing to summarize our meeting. Mary, I'm copying you because I wanted you to know what we agreed upon yesterday."

Cc for CYA

Bad Idea: Maybe you're not really sure if you're on the right track, so you copy your boss, figuring that this will give her an opportunity to correct you if she doesn't agree with your course of action. See above. She's probably not reading it, and copying her does not absolve you of responsibility anyway. This is another source of communication breakdown within an organization, sometimes with damaging results.

Better: Run your intentions by your boss prior to the communication. Or, as above, address your boss directly in the message and invite her input. For example: "Jane, I think we should go with the 5×7 flier. Mary, please let me know if you disagree."

Bcc for Private Communication

Bad Idea: You've probably heard at least one horror story about a Bcc gone embarrassingly awry. A common use for bcc is to share a message with someone that you don't want the recipient to know you shared. Ethics aside, there is simply too much potential for unintended consequences with a bcc.

Better: If you want to privately copy someone on a message, send it to the primary recipient, then go into your "sent" folder and forward the message, alerting the "private" recipient why you are sending it to them. For example, "Mary, below is the message I sent to Jane to call attention to her frequent tardiness