SOP Number 0011

SOP Title Confidentiality and Open Access

	NAME	TITLE	SIGNATURE	DATE
Author	Verita Barton	Head of Quality Assurance		19/11/19
Reviewer				
Authoriser	Verita Barton	Head of Quality Assurance		

Effective Date:	19/11/19
Next Review Date:	01/09/20

READ BY			
NAME	TITLE	SIGNATURE	DATE

1. PURPOSE

This Standard Operating Procedure is designed to complement the existing '*Privacy*' policy and *'Data Protection'* policy and should be read in conjunction with these documents. It will provide a framework of how Upward Mobility handles, stores, and accesses personal data.

2. INTRODUCTION

Those using Upward Mobility's services, or who are in employment of Upward Mobility (whether in a paid or voluntary capacity), have the right to expect that any information shared by them with the charity will be used solely for the purpose for which it is given and will remain within the organisation. Upward Mobility will always endeavour to ensure that trust and confidence in the charity is upheld at all times and that all students, families/carers, and staff are treated with dignity and respect. This principle extends to any information about the internal affairs of Upward Mobility.

Upward Mobility also recognises the right of students, staff and volunteers to have open access to their personal records held by the charity.

3. DEFINITIONS

N/A

4. LEGISLATION

When The following legislation contributes to the regulation of confidentiality and open access:

- The Human Rights Act 2000 guarantees respect for a person's private-and family life, their home and correspondence.
- The General Data Protection Regulation 2018 (GDPR) protects the rights and privacy of individuals and covers personal information - which includes facts and opinions about an individual that might identify them. The purpose of this regulation is to ensure that data about an individual is not processed without their knowledge, is processed with their consent wherever possible, and is kept securely at all times.

5. PROTECTING CONFIDENTIALITY

Upward Mobility is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

At Upward Mobility, confidentiality implies that information is given to the organisation and not to an individual. Therefore, information is not confidential to the person who receives it, but to the organisation as a whole and can be disclosed within the organisation on a 'need to know' basis, as and when required. Thus, only the information a staff member needs to know in order to do their job properly and safely is released. In addition to this, information will not be released to a third party without the permission of the person concerned, unless one of the following exceptions applies:

- Disclosure is required by law (i.e. acts of terrorism are suspected).

- Where these is a reasonable belief that there is concern that the health and safety or welfare of an individual is at risk.

In such cases, the information must be disclosed to the Head of Service Delivery, who will review and determine the appropriate action. The minimum amount of disclosure possible will be expected in any such situation by anyone involved.

In order to protect confidentiality, Upward Mobility will do the following:

- Permission is sought to collect information and people will be informed of their right to access this information. This includes notifying students, staff and volunteers that data is held, why it is held and that they are entitled to access it.
- Permission for photography, filming, use of social media, etc. have been gained through the completion of 'Permission form 1' as an appendix to the student contract – covering the use of photographs in any publication, newsletter or leaflet. It also covers the use of photographs or films on Upward Mobility's social media sites. Similarly, a permission form covering the use of photos/films in all of the abovementioned instances, get completed by all staff. No photograph will be used unless every person in a photograph has given their permission for the photograph to be used in that particular instance. Similarly, no photographs will be used on Upward Mobility's website or social media sites unless every person in a photograph has given their permission for the photograph to be used in that particular instance.
- Information will only be collected when it is necessary for a specific purpose. Therefore, Upward Mobility will be clear on why data is collected, data will not be collected without a specific purpose in mind, and it will only be used for the purpose indicated.
- Information and data held will be maintained appropriately. Therefore, data will not be retained longer than necessary - it will only be obtained appropriately, and it will be kept up to date as appropriate.
- If information is to be released to a third party, permission must be sought unless one of the exceptions listed above apply. This is in respect of students, staff and volunteers. Permission may be sought verbally, or it may be necessary to obtain permission in writing.
- Information records will be stored securely in order to observe the provisions of the GDPR, and to prevent unauthorised access. This will be done in line with Upward Mobility's *Data Protection* and *Privacy* policies.
- Consideration will be given to the physical environment in which information is exchanged in order to ensure confidentiality. Calls of a confidential nature should be taken in a secure environment and care must be taken when using emails, printers, faxes, photocopiers, etc.
- Documents which contain identifying information must be handled, stored and disposed of securely and strictly in accordance with agreed organisational procedures, as well as relevant legislation.

- Permission must be gained before publishing case studies (i.e. for publicity, or in training-or information materials). Alternatively, anonymised case studies may be used for these purposes, but details must be sufficiently altered so that it will not be possible for an individual to be thus identified.
- All computers used to process student and staff documentation must be password protected and a 'screen lock function' must be in use when the computer user is away from their desk.
- Any office space located at sites other than Links House, must be locked when the office is unattended.
- In the event that students ask about confidentiality or indicate that they are about to disclose information of a highly sensitive nature, they should be made aware of Upward Mobility's procedure for *Confidentiality and Open-Access*, as well as Upward Mobility's *Adult Support and Protection* policy – which deals with the disclosure of sensitive information. Students can request a copy of these documents, or request to view the documents at any time.

In addition, the following guidelines must be adhered to by all staff in order to ensure compliance with Upward Mobility's *Data Protection* policy:

- All student support documentation (which includes but are not limited to support plans, risk management forms, medical forms, ILPRs, new student information, taster feedback forms, contact detail sheets, student reports pertaining to accidents and incidents, seizure record forms, Outward Mobility support folder, etc.) must be kept locked away in in the designated locked filing cabinets. Student support documentation must be accessed in line with the standard operating procedure outlined in this document.

- In the event that student information is needed by a case manager for a student, or by a member of the management team, it must be ensured that the information is not left unattended during working hours. Information must also not be left within a locked office-space after working hours. It is the responsibility of the manager/designated member of the operational team dealing with the student information (which includes but are not limited to support plans, risk management forms, medical forms, ILPRs, new student information, taster feedback forms, contact detail sheets, student reports pertaining to accidents and incidents, seizure record forms, Outward Mobility support folder, etc.) , to return the information to the designated filing cabinet **at the end of each working day** (a working day will also include weekend days where work was done that required access to student support information)– regardless of whether a task relating to the information, has been completed or not. In the event that information was taken to another Upmo site for use in a student review, it is the responsibility of the case manager to ensure that the documents are signed out of the designated cabinet, kept securely at all times, and returned and signed back in to the designated filing cabinet at the earliest opportunity.

- All staff information (which includes but are not limited to staff records/supervision minutes, names and addresses, references, different types of correspondence, etc.) must be kept locked away in designated locked filing cabinets at all times. Staff files

must be accessed in line with in line with the standard operating procedure outlined in this document.

- All staff files and confidential staff information must be not left unattended during working hours. Information must also not be left within a locked office-space after working hours. It is the responsibility of the manager/designated member of the operational team dealing with the staff information, to return the information to the designated filing cabinet **at the end of each working day** (a working day will also include weekend days where work was done that required access to student support information)– regardless of whether a task relating to the information, has been completed or not. In the event that information was taken to another Upmo site for use in a meeting with a member of staff, it is the responsibility of the manager to ensure that the documents are signed out of the designated cabinet, kept securely at all times, and returned and signed back in to the designated filing cabinet at the earliest opportunity.

- Upward Mobility staff are required to submit ILPRs or 1-1 reports for students that attend their workshops/that they support. In the unlikely event that a staff member types an ILPR on their own personal/shared computer/other electronic device, the staff member must ensure that the ILPR/1-1 report is deleted off of their personal/shared computer/other electronic device after it has been emailed to the Quality Assurance team. **Failure to do so is a breach of Upward Mobility's *Data Protection* Policy.**
- In the event that a member of staff uses an Upward Mobility laptop/electronic device to write an ILPR/1-1 report, they must ensure that the ILPR/1-1 report is deleted from the laptop/electronic device after it has been emailed to the Quality Assurance team. **Failure to do so is a breach of Upward Mobility's *Data Protection* Policy.**

- Student Medication Administration Records (MARs sheets), student medication support plans, and first aid forms must be kept in a locked filing cabinet within the Team Leader office/Team Leader desk at all times. Team Leaders/a designated member of the operational team will access this information when needed, and will ensure that it is securely locked away in the designated locked filing cabinet after each use.

- All person-identifiable information must be destroyed securely by shredding it.

- Upward Mobility staff uses film/photographic data/sound recordings as part of the curriculum within certain workshops. Upward Mobility has designated cameras, camcorders, and laptops to use for this – which are stored in a locked cabinet. It is the responsibility of the staff member to ensure that these electronic devices are signed out from and returned following the correct procedure. Staff must ensure that electronic devices are not left unattended whilst in use. Electronic devices must not be removed from Upward Mobility premises, unless it has been agreed with Upward Mobility management. Staff members must not use their own personal electronic devices (personally owned storage devices such as USB or data sticks, external hard drives, tablets/iPads, computers, mobile phones, personal digital cameras, or MP3 players) to photograph/film/record students – unless it is immediately down-loaded onto a designated Upward Mobility electronic device and then deleted from the staff member's own electronic device.

- Photographic and video recordings made for educational purposes form part of a student's assessment and record of time spent at Upward Mobility. Although consent to certain recordings, such as films made within workshops, can be agreed in the student's appendices to their contract, Upward Mobility staff should always ensure that they make clear in advance what photographic or video recording output will result from that process, and all relevant parties are informed.

- Photographic and video recordings that are made for any purpose of an Upward Mobility workshop or event cannot be used for any purpose other than those stated within the contract for use. Staff cannot display them at outside events unrelated to the workplace in any circumstance. Staff cannot take any images or video recordings home with them and are not allowed to transfer any images onto personal equipment.

- Upward Mobility recognises that some staff may opt to receive their work-related emails on their mobile phones. Some work-related emails may contain confidential information about students and are intended to be viewed by the recipients only. It is therefore the responsibility of each Upward Mobility employee using their mobile phone to receive work-related emails, to ensure that their mobile phone is password-protected at all times.

6. MANAGEMENT OF STUDENT AND STAFF FILES AND ACCESS TO FILING CABINETS

The term **designated office staff** (in the case of student files) will refer to members of the senior management team, the Quality Assurance team, the finance team, Team Leaders, and student case managers. In the case of project worker staff files, **designated office staff** will refer to members of the senior management team, the Quality Assurance team, the finance team, and Team Managers.

1. ONLY **designated office staff** are to use the keys to open the filing cabinets to take out any files.
2. If a member of staff requires access to a student file, they have to request the file from **designated office staff,** who are to unlock the cabinets personally, take the requested file out and hand it to the member of staff.
3. Once the staff member is finished reading the file, the file must be handed back to the **designated office staff** for filing.
4. The keys to the filing cabinets **are not** to be given to non-designated staff under any circumstances.
5. The keys are kept in a locked keysafe (one for staff files and one for student files), and the combination to a keysafe is only known to **designated office staff.**
6. Confidential filing cabinets must be kept locked at all times when the cabinets are not in use. Keys must never be left in the lock of the filing cabinet, and keysafes must never be left unlocked.

7. When a student/staff file is taken out for use, the **designated office staff**, should indicate this on the sign-out sheet provided.

In addition to this, operational staff files are kept in a separate filing cabinet and access to these files are restricted to members of the senior management team, and two administrative assistants only. Keys for this filing cabinet are kept by members of the senior management team, and can only be handed to the two administrative assistants upon request – in line with their organisational duties.

7. DISPOSAL OF CONFIDENTIAL INFORMATION

All confidential information (including information that only contains names), should be shredded. It should not just be disposed of in the paper recycling containers.

8. OPEN ACCESS TO PERSONAL RECORDS

Students, staff and volunteers may request access to their personal records. This can include access to student reports, case notes, staff records such as files notes and minutes, etc.

The request should be made in writing to the head of service delivery and access should be provided as soon as possible, but within a maximum of 40 days (the statutory maximum) and usually within 20 days. Students can be assisted by a member of staff, to put their request in to writing.

Information obtained in confidence from a third party (including references provided during recruitment) should not be disclosed without the consent of the third party.

In exceptional circumstances, sensitive information may need to be withheld. Exceptional circumstances may include (but are not limited to) case notes from a closed section (a part of the meeting not attended by the student) of an adult support and protection case conference, or a student report of a sensitive nature that includes confidential information pertaining to another student, a complaint made by a staff member who wish for their anonymity to be protected, etc. Any decision to withhold information must be taken by the senior management team.

The need to withhold access to sensitive items within the records should never be used to justify withholding access to the remainder of the information.

9. IMPLEMENTATION

All staff and volunteers will receive training and support to help them understand the policy and to implement it. They will be made aware of the serious nature of a breach of confidentiality. In certain circumstances (i.e. operational staff processing pay records or having access to staff files), staff may be asked to sign a confidentiality agreement.

If there are any concerns regarding the application of the policy, the following should be done:

- Staff should speak to their line manager.

- Volunteers should contact the Team Leader who is their designated point of contact, and the Team Leader will liaise with their own manager.

10. FORMS/TEMPLATES TO BE USED

N/A

11. INTERNAL AND EXTERNAL REFERENCES

11.1 Internal References

Data Protection policy

Adult Support and Protection policy

Privacy policy

11.2 External References

General Data Protection Regulation 2018 (GDPR)

Data Protection Act 1998

Human Rights Act 2000

12. CHANGE HISTORY

SOP no.	Effective Date	Significant Changes	Previous SOP no.
0011	**19/11/19**	**FIRST EDITION**	**N/A**