RAINBOW HUB
E-Safety
Policy & Procedure (including Mobile Phones and Remote Therapy)

1.0 INTRODUCTION

ICT and online resources are increasingly used in many areas of life, including here at Rainbow Hub, including the internet, social media and mobile devices. This e-safety policy should be read in conjunction with other Rainbow Hub policies including; Safeguarding and Child Protection Policy; Safeguarding and Protection of Adults at Risk Policy; Working from Home Policy; Data Protection Policy and Confidentiality Policy.

2.0 POLICY STATEMENT

Rainbow Hub works with children and families in providing its services and has a commitment to look after their welfare, keep them safe from harm and protect their privacy- this includes having policies and procedures in place for the safe use of: email; internet; Rainbow Hub network, equipment and data; digital images and digital technologies including mobile phones and digital cameras; social media; publication of beneficiary information/ photographs on the website and social media; the delivery of remote therapy.

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of beneficiaries is paramount when beneficiaries, staff, students, volunteers and visitors are using the internet, social media or mobile devices and the above technologies and media.
- Provide staff, volunteers, students and visitors with the overarching principles that guide our approach to online safety.
- Ensure that, as an organization, we operate in line with our values and within the law in terms of how we use online devices.

The policy applies to all staff, volunteers, beneficiaries, parents/carers, visitors, contractors and anyone involved in Rainbow Hub's activities. This includes the use of personal devices by all of the above mentioned groups such as mobile phones or iPads/tablets which are on or brought into the setting. This policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site, such as a work laptop, iPad or mobile phone.
For the purposes of this policy 'beneficiary' includes all children, young people and adults accessing services at Rainbow Hub.
The policy applies to all services provided by Rainbow Hub including all therapy services, nursery and school provision.

The implementation of this policy will ensure a suitable framework exists within the organisation to manage risks associated with the above technologies and social media whilst also harnessing the opportunities it provides for communication, promotion, marketing etc.
In order to meet this policy the particular arrangements which we will make are set out within this document and sufficient resources will be made available to honour our commitment to the policy.
The policy will be kept up-to-date, particularly as the setting changes in nature and size and will be revised annually, or as and when required. We therefore welcome any useful comments from members of staff, parents/carers, beneficiaries, volunteers, students, supporters, partners and visitors regarding this policy.

3.0 EMAIL USE

The setting provides all staff with access to a works email account to use for all work related business, including communication with parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with beneficiaries and their families.

All emails should be professional in their tone and checked carefully before sending, just as an official letter would be.

Email is covered by the Data Protection Act (2018) and the Freedom of Information Act (2000) so safe practice should be followed in respect of record keeping and security. All staff are aware that all email communications may be monitored at any time to monitor acceptable use. All users must report immediately any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature, to their line manager.

All emails that go through the Rainbow Hub server will be cached for 30 days before being permanently deleted.

4.0 USE OF SOCIAL NETWORKING SITES/SOCIAL MEDIA

The charity publishes information about Rainbow Hub services and communicates with beneficiaries/parents/carers/supporters in many ways.

- Formal and informal meetings
- Newsletters
- Emails and text messages
- Our own website
- Social media

The charity welcomes anyone who is interested in the work of Rainbow Hub to follow us and connect with us on the various media sites that the charity uses. At present that includes - Twitter, Facebook, Instagram, YouTube, Google+. These sites allow the charity to communicate about the day-to-day life of the organisation and give notice of forthcoming events and activities.

4.1 SOCIAL MEDIA SITES

It is important for everybody's safety that we are clear about how we use these sites, and what is acceptable behaviour from people who choose to follow us.

We use our social media sites to publish information that is of general interest. We do not believe it is an appropriate place to discuss personal matters specific to individual members of our community, whether that be users, families supporters or staff.

4.2 PRIVACY

- We will not publish photographs of beneficiaries without completion of a consent form.
- We will not identify by name any beneficiary published on our social media accounts without the written consent of parents/carers or (if appropriate) the adult beneficiary themselves.

4.3 RESPECT

- We will not tolerate any form of bullying or discrimination on our social media accounts.
- We will not allow posts or comments that refer to the specific individual or group matters between the charity and members of its community.
- We will not tolerate any comments or posts that are defamatory, rude or abusive towards any member of our community, whether that is children, families, supporters, staff or trustees.

4.4 OUR RULES

Rainbow Hub recognises the importance of social media in the modern world however steps must be taken to protect the organisation and its staff from potential incidents arising from its use.

4.5 RAINBOW HUB ACCOUNTS

The Fundraising team represent Rainbow Hub by handling corporate social media accounts or speak on behalf of the charity. When doing so, we expect staff to act carefully and responsibly to protect the image and reputation of Rainbow Hub.

Staff who are given access to post on our social media accounts should:

- **Be respectful, polite and patient,** when engaging in conversations. Staff should be extra careful when making declarations or promises towards stakeholders.
- **Avoid speaking on matters outside their field of expertise** when possible. Staff should be careful not to answer questions or make statements that fall under somebody else's responsibility.
- **Follow our Confidentiality Policy and Data Protection Policy** and observe laws on copyright, trademarks, plagiarism and fair use.
- **Inform Head of Fundraising or CEO** when about to share any major-impact content.

- **Avoid deleting or ignoring comments** for no reason. They should listen and reply to criticism.
- **Never post discriminatory, offensive or libellous** content and commentary.
- **Correct or remove** any misleading or false content as quickly as possible.
- **Take care with the presentation of content.** Make sure there are no typos, misspellings or grammatical errors. Check quality of images.
- **Content about supporters or service users** should not be posted without their consent
- **Accounts must not be set up on any social media channels** on behalf of Rainbow Hub. This can lead to confused messaging and brand awareness.
- **Rainbow Hub is not a political organisation** and does not hold a view on party politics or have any affiliation with or links to political parties.
- **If any staff outside of the Fundraising team** become aware of any comments online that may affect Rainbow Hub and become a crisis, they should speak to the CEO or a senior manager.

4.6 GUIDANCE FOR PERSONAL ACCOUNTS

This policy does not intend to inhibit personal use of social media but flags up areas in which conflicts might arise.

In order to safeguard the charity and its employees, Rainbow Hub staff should not personally connect with any child, parent or beneficiary of Rainbow Hub via any of the social media platforms. Any contact through social media should be done via the charity accounts as referred to at paragraph 4.5

Staff can access their personal accounts during working hours for work related matters however we expect staff to act responsibly and ensure productivity is not affected.

Rainbow Hub staff can interact with supporters and volunteers of Rainbow Hub but must apply caution when doing so using their personal 'profiles' and be mindful that it could compromise the professional image of the organisation and the staff member. It could also create confusion around what is an 'appropriate' professional relationship. Staff should remember that they have a duty to safeguard not only themselves but the charity itself. Staff are also expected to adhere to the Confidentiality Policy at all times.

We advise our employees to avoid any defamatory, offensive or derogatory content. It may be considered as a violation of our company's anti-harassment policy, if directed towards internal or external stakeholders.

Be mindful of your own privacy and safety online and always protect yourself and Rainbow Hub. What you publish is often more widely accessible than may be apparent and will be around for a long time.

Any member of staff who has/or decides to start a personal blog or website which indicates that they work at Rainbow Hub should discuss any potential conflict of interest with the CEO/Senior Manager.

Be aware of copyright laws which can affect the reproduction of printed materials and images if used without the appropriate licence or agreement. Never use or adapt someone else's images or written content without permission. Failure to acknowledge the source/author where permission has been granted can also be considered a breach of copyright.

Staff who may be politically active must be clear in ensuring their personal views are not associated with Rainbow Hub as the charity is non-political.

Rainbow Hub logos can only be used with the approval of the Fundraising team.

4.7 COMMENTS

Where allowed by the social media site, we welcome comments on the information we post. However, we reserve the right to delete comments and ban further comments from anyone who causes offence to others or makes inappropriate remarks that could damage the reputation of Rainbow Hub.

5.0 MOBILE DEVICE USE AND RECORDING (INCLUDING PHOTOGRAPHS AND VIDEO)

5.1 INTRODUCTION

Since nearly all mobile devices now have camera, video and audio recording capacity the use of recording devices is an inevitable part of modern daily life.

The use of mobile devices within Rainbow Hub must be carefully considered in order to balance the need to safeguard the welfare of our beneficiaries with the desire and/or requirement to capture footage or images to record and monitor.

A mobile device is a portable, wireless computing device that is small enough to be used while held in the hand. Most commonly these are laptop computers, tablets and mobile phones. This policy will also discuss the use of wearable devices that can be synced with mobile devices (i.e. watches).

5.2 MOBILE DEVICES IN THE SETTING

Inevitably most people that come into Rainbow Hub in whatever capacity will have a mobile device with them on arrival in the setting. In order to safeguard the beneficiaries Rainbow Hub has guidelines in place to monitor/control the setting.

5.2.1 STAFF GUIDELINES (including volunteers & students)

- Rainbow Hub allows staff to bring in personal mobile phones and devices for their own use. These must be stored in the designated storage areas on arrival (in lockers or in the office where a locker is not available) and must not be retrieved during session times without consent of their line manager. Staff will sign in to confirm their adherence to this on arrival each day.

- Rainbow Hub is not responsible for the loss, damage or theft of any personal mobile device.
- Staff must not have personal mobile devices within the classroom or in the nursery rooms at any time.
- Mobile telephones, cameras or other photographic/audio equipment other than those belonging to the charity, must not be taken into areas where beneficiaries are present or accompany staff when they are on outings.
- Staff may wear wearable devices (i.e. watches) in the classroom however the functionality of these must be set to silent/no notifications so that they are not distracting to staff during their work.
- Staff must not use their personal mobile devices during work hours except in emergency situations
- If staff wish to use their personal mobile devices during breaks/lunch hours etc., they may do so in 'public' areas on the site (i.e. not in classrooms, nursery rooms or outdoor play areas).
- No staff member in the setting is permitted to record audio or visual footage of service-users on their personal mobile device when in the setting.
- Staff will not be able to claim any payment for the use of personal mobiles on work issues unless authorised in advance by the CEO.
- Where Rainbow Hub provides mobile technologies such as phones, laptops or iPads for offsite visits and trips and offsite working , only these devices should be used and this policy must be observed at all times
- When such devices are allocated to employees this will be done by their line manager and serial numbers recorded.
- When using such devices working from home, Rainbow Hub's Working from Home Policy must be observed at all times.
- Rainbow Hub's devices should only be used in the classroom when authorised by a line manager. They should be locked away when not in use and should be locked away overnight.

5.2.2 PARENT/CARER/ADULT SERVICE-USER GUIDELINES

- Parents/carers/adult beneficiaries may have personal mobile devices on their person anywhere in the setting.
- However, the functionality of these must be set to silent/quiet so that the distraction they cause can be kept to an absolute minimum.
- Should a parent/carer/adult beneficiary wish to use their personal mobile devices they will be asked to do so in 'public' areas on the site (i.e. not in classrooms, nursery rooms, offices or outdoor play areas).
- Should parent/carer/adult beneficiaries wish to record themselves or the beneficiary, they are permitted to do so only if they abide by the following precautions:
    - Verbally check with staff that may appear in the footage that they consent to being recorded and for subsequent sharing e.g. on social media.

- Ensure that no other people (e.g. other beneficiaries, visitors, other parents etc.) are recorded – even in the background - without verbal consent to being recorded and for subsequent sharing e.g. on social media.
- Ensure that no other identifying information (e.g. children's photos on wall, number plates on cars) are recorded – even in the background.

5.2.3 OTHER PEOPLE IN THE SETTING

- Visitors, supporters and other people coming into the setting may have personal mobile devices on their person anywhere in the setting where supervised by a member of staff.
- However, the functionality of these must be set to silent/no notifications so that the distraction they cause can be kept to an absolute minimum.
- Should a Visitor/supporter/other person wish to use their personal mobile devices they will be asked to do so only in 'public' areas on the site (i.e. not in classrooms, nursery rooms or outdoor play areas).
- No visitor/supporter/other person in the setting is permitted to record audio or visual footage when in the setting. If they require an image e.g. a cheque presentation then Rainbow Hub will use the setting's recording devices and then share in line with the setting's media permissions.

5.3 CLASSROOM RECORDING AND MONITORING

- For monitoring and assessment purposes it is necessary for the classroom staff to record images, audio and footage of the beneficiaries.
- It is also necessary to record images, audio and footage of the beneficiaries for marketing, publicity, fundraising etc.
- We ensure that any recordings taken of beneficiaries in our setting are only done with prior written permission from each child's parent/carer or the adult beneficiary themselves or their care worker.
- This permission is requested when each beneficiary enrols in the setting and is updated on an annual basis to ensure that this permission still stands (Media Permissions Form).
- If a parent/carer/adult beneficiary is not happy about one or more of the uses of recordings then the setting will respect their wishes and find ways to ensure we are still able to record the individual's progress.
- Staff are not permitted to take photographs or recordings of a beneficiary on their own devices and only use those provided by the setting. The Service Lead/Senior Conductor and nominated officers will monitor all photographs and recordings to ensure that the parents/carers/adult beneficiary's wishes are adhered to.
- The setting has classroom and office-specific recording devices that are available for recording and monitoring (currently tablets & cameras are used). These should only be used in the classrooms when authorised by a line manager. They should be locked away when not in use and should be locked away overnight.
- **Location of Cameras/Recording Devices for the therapy classrooms at Rainbow Hub is:** Within the Hub Office in a lockable drawer which is locked at the end of each day.

- **Location of Cameras/Recording Devices for the office/fundraising at Rainbow Hub is:** Within large filing cabinet in fundraising office which is locked at the end of each day.
- **Location of Cameras/Recording Devices for the Nursery at Rainbow Hub is:** Within the Nursery Office in a lockable drawer which is locked at the end of each day.
- **Location of Cameras/Recording Devices for the School at Rainbow Hub is:** Within the School Office in a lockable drawer which is locked at the end of each day.

- Memory cards must remain on the premises when they are not being used.

- **If the recording device has access to social media these sites/functions MUST NOT be used within the classroom at any time. If Rainbow Hub social media is accessed via the device then it must be logged in and out each time it is used on each device and NEVER logged into whilst in the classroom spaces.**

5.4 STORAGE and SHARING OF IMAGES/RECORDINGS

- Only permitted staff will be allowed to upload photographs and this will be on a weekly basis to the network storage and then deleted from the devices (the Service Lead/Senior Manager and/or Nominated Officer will monitor all images/recordings).
- If images are to be shared publically (e.g. on social media) this can be done directly from the recording device if this functionality exists. However, this MUST NOT BE DONE within the classroom spaces during session times.
- Images should be transferred to a child's file and removed from the device. The device should not contain images longer than necessary but certainly no more than one week.
- NB. For details of the procedure for ongoing storage of images/recordings within the setting please refer to the Data Protection Policy and Procedure.

6.0 LAPTOPS/IPADS/TABLETS

Staff Use:

- Where staff have been issued with a device for work purposes, personal use off site is not permitted unless authorised by their line manager. The settings laptops/ iPads/ devices should be used by the authorised person only.
- Staff are aware that all activities carried out on setting devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy.
- Staff will ensure that setting laptops and devices are made available as necessary for anti-virus updates, software installations, upgrades or routine monitoring/ servicing.
- Setting issued devices only should be used for this purpose and if containing sensitive information or photographs of beneficiaries, should not leave the premises unless password protected.

Beneficiary Use:

- Laptop/ iPad use must be supervised by a member of staff at all times.
- Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Beneficiaries should not be able to search or install anything on a setting device.
- Beneficiaries may bring in their own devices for communication purposes. Their parent/carer or the adult beneficiary where appropriate, must ensure there is no inappropriate or illegal content on the device.

7.0 APPLICATIONS/ SYSTEMS FOR RECORDING BENEFICIARIES' ATTENDANCE/ PROGRESS

There are several apps which allow staff to track and share a child's progress online with parents/ carers, usually in the form of photographs and text. Such tools have considerable benefits, including improved levels of engagement with parents and a reduction in paperwork. There are also systems allowing beneficiaries progress and attendance to be monitored. Careful consideration must be given to safeguarding and data security principles before using such tools.

Personal staff mobile phones or devices (eg iPad or iPhones) should not be used for any apps or systems which store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately password protected. This is to prevent a data security breach in the event of loss or theft.

8.0 REMOTE THERAPY AND ONLINE COMMUNICATION

8.1 Information and guidance regarding remote learning during Covid-19:

- DfE 'Safeguarding and remote education during coronavirus (COVID-19)'
- The Education People:' Safer remote learning during Covid-19: Information for School Leaders and DSLs'
- SWGfL: Safer Remote Learning
- LGfL: Coronavirus Safeguarding Guidance
- NSPCC: Undertaking remote teaching safely
- Safer Recruitment Consortium: 'Guidance for safer working practice for those working with children and young people in education settings Addendum' April 2020

This section should be considered alongside other Rainbow Hub policies including:

- Confidentiality Policy
- Working from Home Policy
- Data Protection Policy.
- Safeguarding and Child Protection Policy
- Safeguarding and Protecting Vulnerable Adults Policy

8.2 Leadership Oversight and Approval

- Remote therapy sessions will only take place using Zoom. Zoom has been assessed and approved by the CEO

- Staff will only use Rainbow Hub managed or specific, approved professional accounts with beneficiaries and parents/carers.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted. Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the CEO.
- Staff will use equipment provided by Rainbow Hub at all times when delivering remote therapy sessions.
- All remote lessons will be formally timetabled; a member of the Senior Management Team can join at any time.
- Live streamed remote learning sessions will only be held with approval and agreement from the CEO.
- All online sessions should be risk assessed and appropriate measures put in place.

8.3 Data Protection and Security

- Any personal data used and captured by staff delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
- All remote learning and any other online communication will take place in line with current confidentiality expectations as outlined in our Confidentiality Policy.
- All participants will be made aware that they cannot record therapy sessions without the express permission of the lead therapist.
- Any recordings that are taken should be viewed by the therapist before videos are placed on social media.
- Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by the Senior Management Team and in line with our Data Protection Policy requirements.
- Only staff of Rainbow Hub will be given access to the network server.
- Access to the network will be managed in line with current IT security expectations.
    - All sensitive information is protected by a password which should not be given to anyone from outside the organisation.

8.4 Session Management

- Staff will record the length, time, date and attendance of any sessions held and details will be kept on the daily registers.
- Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - Not permitting beneficiaries to share their screens
    - Ensuring a waiting room is used
- When live streaming with beneficiaries:
    - contact will be made via Rainbow Hub provided email accounts and/or logins.
    - contact will be made via a parents/carer account.
    - staff will mute/disable beneficiaries' videos and microphones at any time their behaviour becomes inappropriate.
- A pre-agreed email detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Beneficiaries should not forward or share access links.

- Beneficiaries should attend sessions in a suitable space and be appropriately supervised by a parent/carer.
- Only the beneficiaries and known parent/carers should be present during group sessions.

8.5 Behaviour Expectations

- Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
- All participants are expected to behave in line with existing policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
    - Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.
- Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
- If sharing videos and/or live streaming, staff are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

8.6 Policy Breaches and Reporting Concerns

- Staff and beneficiaries are encouraged to report concerns during remote and/or live streamed sessions to the CEO or Designated Safeguarding Lead.
- If inappropriate language or behaviour takes place, those involved will be removed by staff, the session may be terminated, and concerns will be reported to the CEO.
- Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
- Sanctions for deliberate misuse may include restricting/removing use, allegations of misconduct, and contacting police if a criminal offence has been committed.
- Any safeguarding concerns will be reported to Joanne Ashcroft, Designated Safeguarding Lead, in line with our Safeguarding and Child Protection Policy.

9.0 DATA STORAGE AND SECURITY

Rainbow Hub's Data Protection Policy must be followed at all times.

In line with the requirements of the Data Protection Act (2018), sensitive or personal data is recorded, processed, transferred and made available for access in the setting and in limited circumstances outside of the setting as permitted above. This data must be accurate; secure; fairly and lawfully processed; processed for limited purposes and in accordance with the data

subjects rights; adequate, relevant and not excessive; kept no longer than necessary; and only transferred to others with adequate protection.

At Rainbow Hub we specify how we keep data secure and inform staff as to what they can/cannot do with regard to data through this e-Safety policy, our Data Protection Policy and our Records Management and Retention Policy. Lyndsay Fahey, Karen Williams and Joanne Ashcroft are responsible for managing information.
ICT enables efficient and effective access to and storage of data for the management team, staff and administrative staff. Only trained and designated members of staff have authority and access rights to input or alter data.

The centre has defined roles and responsibilities to ensure data is well maintained, secure and that appropriate access is properly managed with appropriate training provided.

The files and network system are backed up daily so that copies of the data will always be available. Where an allegation is made or an incident reported Rainbow Hub will attempt to retrieve browsing history using third party recovery software where deemed necessary.

Approved anti-virus software is updated regularly on all IT (ipads /laptops etc). All laptops and computers are password protected. All work email accounts are password protected. Staff should not share their passwords with anyone; write their passwords down or save passwords in web browsers if offered to do so. Staff should not use their username as a password. Staff should not email their password or share it in an instant message. Staff should change their password if they think someone may have found out what it is.

Staff should be aware of who they are allowed to share information with. Clarification can be obtained from the CEO.

Staff should only download files or programs from trusted sources.

Staff should lock sensitive information away when left unattended. Unauthorised people should not be allowed into staff areas. Computer screens should be positioned so that they cannot be read by others who shouldn't have access to that information. Confidential documents should not be left out.

Staff should only take information offsite when authorised and only when necessary. On occasions when this is necessary, staff should ensure that the information is protected offsite in the ways referred to above. Staff should be aware of their location and take appropriate action to reduce the risk of theft. Staff should ensure that they sign out completely from any services they have used, for example email accounts. Staff should try to reduce the risk of people looking at what they are working with. Laptops should not be taken abroad (some countries restrict or prohibit encryption technologies).

10.0 SERIOUS INCIDENTS

If a serious incident occurs such as inappropriate content is accessed, an incident log is made immediately, a nominated officer is informed and appropriate action taken. In such a case our IT provider should be informed immediately with a view to ensuring the pathway is blocked.

11.0 OTHER

Should any other matters arise with regards to the areas covered in this policy then guidance should be sought from CEO/Senior Manager and Services Lead.

Author	Alison Holdsworth
Date approved by Board	20 December 2021
Review Date	27 February 2024
Date Reviewed	27 February 2023
Reviewed By	Alison Holdsworth
Changes made	• Inclusion of definition of 'beneficiary' • Application of policy to all services including school • Inclusion of school office for storage of recording devices/cameras 26/09/23- Addition of Records Management and Retention Policy