Online / E-Safety Policy

Eastern Region Roof Training Group Ltd

Autumn 2019

Prepared by:	*Chloe Smith* *DSL*
Approved by:	*Clive Coote* *Managing Director*
Status & review cycle	Statutory Annual
Date approved:	*08/08/2019*
Review date:	*08/08/2020*

Background / Rationale

Development, monitoring and review of the Policy

Scope of the Policy

Roles and Responsibilities

- National / local organisation / association
- Leaders or Lead Person
- Staff / volunteers
- Children and young people
- Parents and carers

Policy Statements

- Educating children and young people to stay safe on line
- Awareness raising for parents and carers
- Training – staff and volunteers
- Protecting the professional identity of staff and volunteers
- Your technology
- Personal Devices
- How you use technology to communicate
- Use of digital images and video
- Data security
- Unsuitable / inappropriate activities
- Sanctions chart
- Reporting (with flowchart)

Background / Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work with children and young people are bound.

Digital technologies have become integral to the lives of children and young people in today's society. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Children / young people, staff and volunteers have a right to safer internet access at all times.

However, the use of these new technologies can put users at risk. Some of the dangers may include:

- Access to illegal, harmful or inappropriate images or other content

- Loss of privacy / control of personal information
- Grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Hacking, viruses and system security
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other policies (eg safeguarding / child protection policies).

As with all other risks, it is impossible to eliminate the risks completely. By providing good examples / role models and by raising awareness, it is possible to build the resilience of children and young people, so that they have the confidence and skills to deal with these risks.

Groups should be able to demonstrate that they have provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected to manage and reduce these risks. The online safety policy that follows explains how we intend to do this.

Development / Monitoring / Review of this Policy

Should serious online incidents take place, the following external persons / agencies should be informed:	• **Local Authority Child Protection Lead Person or Area Social Work team** • **Local Authority Designated Officer (LADO) (if it involves an allegation against member of staff / volunteer)** • **Police**

Scope of the Policy

This policy applies to all members of ERRTG (including staff, volunteers, children and young people, parents / carers, visitors, community users) who have access to and are users of communications technologies (whether these belong to the group or to the users themselves)

Roles and Responsibilities

Manager:

- The manager Clive Coote has overall responsibility for ensuring the safety (including online safety) of all staff, volunteers and members of the group, though the day to day responsibility for online safety may be delegated to others.
- The manager and Chloe as DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer. (see flow chart on dealing with online safety incidents – included in a later section)
- The manager is responsible for ensuring staff / volunteers receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The manager will ensure that there is a system in place to allow for the monitoring of online safety in the group and that they receive regular monitoring reports.

Staff and volunteers

are responsible for ensuring that:

- they have an up to date awareness of the group's current online safety policy and practices
- they report any suspected misuse or problem to Clive– particularly where it is believed that a child's welfare is at risk.
- digital communications with children and young people should be on a professional level
- they are aware of online safety issues particularly those related to the use of mobile phones, cameras, gaming consoles and hand held devices and that they monitor their use and implement the group policies with regard to these devices

Children and young people:

- **are expected to abide by the Acceptable Use Policy / Rules,** which they are expected to sign before being given access to the organisation's systems and devices
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should demonstrate positive online behaviour

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of communications technologies than their children. ERRTG should therefore take every opportunity to help parents understand these issues

Policy Statements
Educating children and young people to stay safe online

Whilst regulation and technical solutions are very important, their use should be balanced by making children and young people aware of the need to take a responsible approach to online safety. Children and young people need help and support to recognise and avoid online safety risks and build their resilience. Online safety awareness will be provided in the following ways:

- Key online safety messages should be reinforced as part of all relevant planned programmes of activities for young people.
- Online safety issues should be discussed / highlighted, when possible, in informal conversations with young people.
- When the opportunity arises young people should be advised to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Young people should be made aware of the need to respect copyright when using material accessed on the internet and, if applicable, acknowledge the source of information used.
- Rules for the use of devices / internet will be posted in areas where these devices are in use and, where possible, displayed on log-on screens.
- Staff and volunteers should act as good role models in their use of online technologies.

Awareness raising for parents / carers

We should provide online safety information and awareness to parents and carers through:

- Letters, newsletters, web site.
- Meetings with parents / carers (formal and informal).
- Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents) and other relevant resources.

Training – staff and volunteers

It is essential that all staff and volunteers receive online safety awareness training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A planned programme of training about online safety will be made available to staff and volunteers.**
- **All new staff and volunteers will receive awareness training as part of their induction programme, ensuring that they fully understand the online safety policy and acceptable use policies**
- An audit of the online safety training needs of all staff will be carried out regularly

- This online safety policy and its updates will be presented to and discussed by staff and volunteers at staff / team meetings.

Protecting the professional identity of staff and volunteers
This applies to any adult, but particularly those working with children and young people (paid or unpaid) within the group. Consideration should be given to how your online behaviour may affect your own safety and reputation and that of the group.

Communication between adults and between children / young people and adults, by whatever method, should take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites and blogs.

When using digital communications, staff and volunteers should:

- only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of ERRTG
- not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children so as to avoid any possible misinterpretation.
- ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
- not post information online that could bring ERRTG into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.
- E-mail, text or other web based communications between staff / volunteers and a child / young person should take place using ERRTG's official equipment / systems.
- Any communications outside the agreed protocols may lead to disciplinary and/or criminal investigations.

Wider personal use of digital communications:

While the section above refers to communications between staff / volunteers and children / young people consideration should also be given to how the use of digital communications by staff and volunteers in their private lives could have an impact on the reputation of themselves and ERRTG. Everyone should be able to enjoy the benefits of digital technologies. Staff and volunteers should, wherever possible, seek to separate their professional online presence from their online social life and take the following into account when using these digital communications:

- Careful consideration should be given as to who should be included as "friends" on social networking profiles and which information / photos are available to those friends
- Privacy settings should be frequently reviewed.
- The amount of personal information visible to those on "friends" lists should be carefully managed and users should be aware that "friends" may still reveal or share this information
- "Digital footprint" – information, including images, posted on the web may remain there for ever. Many people subsequently regret posting information that has become embarrassing or harmful to them
- A large proportion of employers engage in searches of the internet when selecting candidates and are influenced by the content they find.

Your technology

ERRTG will be responsible for ensuring that all systems and devices will be as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Systems and devices will be managed in ways that ensure ERRTG meets accepted online safety requirements, as below:

- **The use of the internet by children / young people must be supervised and / or monitored**. Guidance will be provided to staff, volunteers, parents and carers on the need for internet access to be supervised
- **Systems and devices will be regularly monitored and users are made aware of this in the Acceptable Use Policy.**
- **Personal data must not be sent over the internet or taken away from the group's offices / facilities unless safely encrypted or otherwise secured**.
- The systems and devices needing protection will be identified. These could be: computers; any device with internet access; networks (hard wired or wireless); TV / media services.
- Devices in use are protected against online security threats, such as: viruses; unauthorised access; spyware and malware.
- The "master / administrator" passwords for the systems / devices must be available to the Leader and another senior person and kept in a secure place (eg a safe).

- An effective filtering system will be used. The filtering will reflect the age, ability and responsibility of the users. There will be regular discussion with all users about filtering to promote wider ownership.
- Requests from staff and volunteers for sites to be removed from the filtered list will be considered by the Leader (or another relevant person). If agreed, this action will be recorded, and logs of such actions shall be reviewed regularly.
- Changes to systems and devices can only be made by those who have permission to do so eg installing software or changing security systems
- Approval to use any removable media (eg memory sticks / CDs / DVDs / games) must be obtained before being used on the group systems and devices.

The following table shows how ERRTG currently considers the benefit of using these technologies outweighs their risks / disadvantages:

	Staff & volunteers				Young people			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff / volunteers	Not allowed	Allowed	Allowed at certain times	Allowed with staff / volunteers permission	Not allowed
Mobile phones								
Taking photos on mobile phones or other camera devices								
Use of hand held devices eg gaming consoles								
Use of the organisation's email for personal emails								
Use of online communication technologies eg social networking, chat rooms, instant messaging, email								

When using communication technologies, the group considers the following as good practice:

- **ERRTG's official email service may be regarded as safe and secure and is monitored.** Staff and volunteers should therefore use only the group's email service, where available, to communicate with others when that communication is related to the group.

- **Users must immediately report, to a nominated person (Clive Coote) the receipt of any communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication.**
- **Any communication between staff / volunteers and the children / young people or their parents / carers must be professional in tone and content.** These communications should, where possible, only take place on official (monitored) systems.
- Young people should be taught about online safety issues, such as the risks attached to the use of personal details. They should also be informed of strategies to deal with inappropriate communications.
- **Personal information should not be posted on the group website and, where possible, only official email addresses should be used to identify members of staff.**

Use of digital and video images

The development of digital imaging technologies has created significant benefits, allowing users instant use of images that they have recorded themselves or downloaded from the internet. However, staff / volunteers and children / young people need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The group will raise awareness about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff and volunteers should raise awareness among children / young people about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- **Written permission from parents or carers will be obtained to allow images to be taken of their children / young people and also allowing their use for legitimate activities or for publicity that reasonably celebrates success and promotes the work of the group.**
- **Parents / carers are allowed to take digital / video images of their children at group special events within the guidelines contained in the Parents / Carers Template Permission Form in the Supporting Policies.**
- Staff and volunteers are allowed to take digital / video images, where appropriate, but must follow the group policies concerning the sharing, distribution and publication of those images. Those images should be taken, where possible, on the organisation's equipment, not the personal equipment of staff and volunteers.

- Care should be taken when taking digital / video images that young people are appropriately dressed and are not participating in activities that might bring the individuals or the group into disrepute.
- If photos are taken, their storage and use must not cause risk or embarrassment.
- Photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images.
- The full names of young people will not be used anywhere on a website, blog, or published article, particularly in association with photographs. Consideration should be given to media coverage and journalists should be made aware of this policy.

Data Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff and volunteers must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- *Transfer personal data using encryption and secure password protected devices.*
- *When personal data is stored on any portable computer system, USB stick or any other removable media:*
    - *the data should be encrypted and password protected*
    - *the device should be password protected (many memory sticks / cards and other mobile devices cannot be password protected)*

- *the device should offer approved virus and malware checking software*
- *the data should be securely deleted from the device, once it has been transferred or its use is complete*

Unsuitable / inappropriate activities

ERRTG believes that the activities referred to in the following section would be inappropriate in a context of working with young people. The group policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for	Unacceptable	Unacceptable and illeg
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					√
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					√
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					√
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					√
	pornography				√	
	promotion of any kind of discrimination				√	
	threatening behaviour, including promotion of physical violence or mental harm				√	

	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the group or brings the group into disrepute				√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards that are in place					√	
Infringing copyright					√	
Revealing or publicising confidential information (eg financial / personal information, computer / network access codes and passwords)					√	
Creating or propagating computer viruses or other harmful files					√	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					√	
Using ERRTG to run a private business						
On-line gaming (educational)						
On-line gaming (non educational)						
On-line gambling						
On-line shopping / commerce						
File sharing (eg Bit Torrent, Limewire)						
Use of personal social networking sites(while "at work")						
Use of video broadcasting eg Youtube						

Sanctions Chart

The group needs to have clear and manageable procedures when dealing with misuse. It is more likely that the organisation will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionately and are recorded and well communicated.

If staff / volunteers suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the “Procedure for Reviewing Internet Sites for Suspected Harassment and Distress” should be followed. This guidance recommends that more than one member of staff / volunteer is involved in the investigation which should be carried out on a “clean” designated computer.

It is intended that incidents of misuse will be dealt with through any accepted disciplinary procedures as follows:

Young People

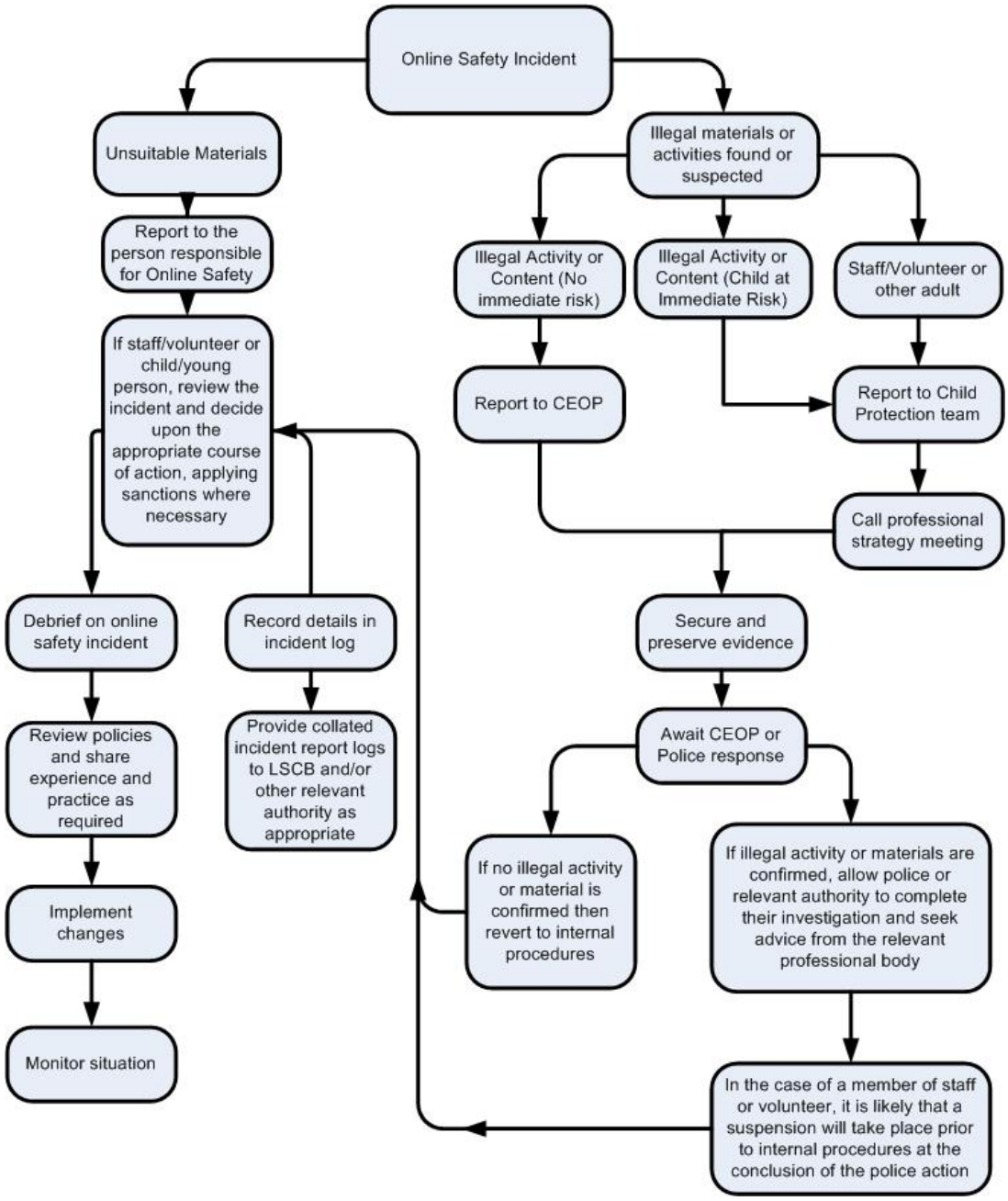
Incidents:	Refer to Leader	Refer to Police	Requires technical response / support	Inform parents / carers	Removal of access to technology / devices	Warning
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	√	√		√		
Unauthorised downloading or uploading						
Allowing others to access technology / devices by sharing username and passwords						
Attempting to access or accessing the technology / devices, using another person's account (hacking)						
Corrupting or destroying the data of other users						
Sending a communication that is regarded as offensive, harassment or of a bullying nature						
Actions which could bring the organisation into disrepute.						
Deliberately accessing materials that the group has agreed is inappropriate						
Activities that infringe copyright or data protection.						
Using proxy by-pass sites or other means to subvert the filtering system						

Staff and volunteers

Incidents:	Refer to line manager / Leader	Refer to National / Local Organisation / body	Refer to Police	Requires technical response / support	Warning	Suspension	Disciplinary action
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	√	√	√				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email "while at work"							
Unauthorised downloading or uploading of files							
Disclosing passwords or any information relating to the security of technology and devices.							
Accidental infringement of the organisation's personal data policy							
Deliberate infringement of the organisation's personal data policy							
Corrupting or destroying the data of other users							
Deliberate damage to hardware or software							
Sending a communication that is offensive, harassment or of a bullying nature							
Using personal communication technologies eg email / social networking / instant messaging / text messaging to communicate with young people (except where allowed in the policy)							
Actions which could compromise the professional integrity of staff / volunteers							
Bringing the organisation into disrepute							
Deliberately accessing materials that the group has agreed is inappropriate							

Breaching copyright or licensing regulations							
Using proxy by-pass sites or other means to subvert the filtering system							
Accidentally accessing materials that the group has agreed is inappropriate and failing to report it.							

Flowchart for responding to online safety incidents



Acceptable Use Policy Agreement
I understand that while I am a member of ERRTG I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the group:

- I will not try to access anything illegal
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within the agreed rules
- I will not deliberately bypass any systems designed to keep the group safer.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the group, without permission.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name _____

Signature _____

Date _____

Template Policies –
Acceptable Use Agreement for Staff and Volunteers

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will act responsibly to stay safer while online, being a good role model for younger users.
- effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
- staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

The term "professional" is used to describe the role of any member of staff, volunteer or responsible adult.

For my professional and personal safety, I understand that:

- I will ensure that my on-line activity does not compromise my professional responsibilities, nor bring my group into disrepute.
- My use of technology could be monitored.
- When communicating professionally I will use the technology provided by ERRTG
- These rules also apply when using the group's technology either at home or away from base.

For the safety of others:

- **I will not access, copy, remove or otherwise alter any other user's files, without authorisation.**
- **I will communicate with others in a professional manner.**
- **I will share other's personal data only with their permission.**
- **I understand that any images I publish will be with the owner's permission and follow the group's code of practice.**
- Wherever possible I will use ERRTG's equipment to record any digital and video images, unless I have permission to do otherwise.

For the safety of the group, I understand that:

- **I will not try to access anything illegal, harmful or inappropriate.**

- **It is my responsibility to immediately report any illegal, harmful or inappropriate incident.**
- **I will not share my online personal information (eg social networking profiles) with the children and young people in my care**
- **I will not deliberately bypass any systems designed to keep the group safer.**
- **I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy** (or other relevant policy). **Where personal data is transferred, externally, it must be encrypted.**
- **I understand that data protection policy requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the organisation's / group's policy to disclose such information to an appropriate authority.**
- **Personal passwords and those of other users should always be confidential.**
- **I will not download anything that I do not have the right to use.**
- **I will only use my personal device if I have permission and use it within the agreed rules**
- **I will inform the appropriate person if I find any damage or faults with technology.**

Staff / Volunteer Name	
Signed	
Date	

Supporting Policy M4

Consent Form for Parents and Carers

A copy of the Children / Young People Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the organisation's / group's expectations of the young people in their care.

Parent / Carers Name:	
Name of Child / Young person:	

As the parent / carer, I give permission for my child to use the group's technology and devices.

I know that my child *has signed an Acceptable Use Agreement and* has received guidance to help them understand the importance of online safety.

I understand that the group will take reasonable precautions to ensure that my child will be safer when online, however, I understand that this manages risk but cannot eliminate it.

I understand that my child's online activity will be supervised and monitored and that ERRTG will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I understand that the group will take appropriate action in the event of any incidents.

I will encourage my child to adopt safe use of the internet and digital technologies.

Signed		**Date**	

Use of Digital / Video Images

The use of digital / video images plays an important part in our activities. Children / young people, staff and volunteers may use digital cameras or other devices to record evidence of those activities. These images may then be used in Learning Journeys and presentations and may also be used to celebrate success through their publication in newsletters, on the website and occasionally in the public media.

The group will comply with the Data Protection Act and request parents / carers permission before taking images of their children. We will also ensure that, wherever possible, full names will not be published alongside images.

It's a great thing to film your child at our events and we know they provide a lot of precious memories. You can support us in keeping our children safe by considering the following:

- Images and video should be for your own or family's personal use only
- Think about privacy and who has the right to see your images, not only of your own child but of others
- If you do share the images online, then you must make sure they are limited to immediate family only and not public
- If you need help in knowing how to do this then come and have a chat with us

Parents / carers are requested to sign the permission form below to allow the group to take and use images of their children.

Permission Form

Parent / Carers Name	
Name of Child / Young Person	

As the parent / carer of the above child, I agree to the group taking and using digital / video images of my child / children. I understand that the images will only be used to support legitimate activities or in publicity that reasonably celebrates success and promotes the work of the group.

I agree that if I take digital or video images at group events which include images of children, other than my own, I will abide by these guidelines in my use of the images.

Signed		**Date**	