E safety policy for The Friendship Café (includes St James City Farm and related projects of the Friendship Café)

Approved : September 19th 2017

To be reviewed on or before 30th September 2018

Roles and Responsibilities

The following section outlines the roles and responsibilities for the online safety of users within the group.

The Friendship Café has relevant online safety / safeguarding policies and guidance. Staff, volunteers and all users should be aware of these guidelines which are included / referred to in this policy document.

Staff, volunteers and users are also governed by relevant legislation, which is referred to in this policy and by the guidance provided by the Local Safeguarding Children's Board (with regard to safeguarding / child protection and how incidents should be reported).

Imran Atcha (Coordinator) 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 Leader (and preferably a deputy) 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 Leader is responsible for ensuring that the Online Safety Lead Person and other relevant staff / volunteers receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. The Leader 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.

Online Safety Lead Person: The Online Safety Lead Person: ensures that

- staff / volunteers have an up to date awareness of the group's current online safety policy and practices,
- all staff / volunteers are aware of the procedures that need to be followed in the event of an online safety incident taking place
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies / documents
- offers advice and support for all users keeps up to date with developments in online safety
- understands and knows where to obtain additional support and where to report issues
- ensures provision of training and advice for staff and volunteers
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,

- communicates with parents and carers
- monitors incident logs

The Lead Person should be trained in online safety issues and be aware of the potential for serious child protection issues.

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 have read, understood and signed the Staff / Volunteer Acceptable Use Policy (AUP)
• they report any suspected misuse or problem to the relevant person 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 and where possible only carried out using the official systems of the group.

• young people in their care are aware of online safety

• 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 may be expected to sign (depending on their age) 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 and 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. The group should therefore take every opportunity to help parents understand these issues (where relevant)

Parents / carers should endorse (by signature) the Acceptable Use Policy for Young People. Parents / carers should sign the relevant permission forms on the taking and use of digital and video images (see appendices)

Educating Young people

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 (not everything on the internet is true or accurate).
- 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.

Inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from any group. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in the context of the care of young people, either because of the age of the users or the nature of those activities.

The group 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:

Unacceptable and illegal

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

Unacceptable

- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm, extremist ideologies or accessing harmful materials or weapons, etc.
- 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
- On-line gambling
- Revealing or publicising confidential information (e.g. 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 the group systems to run a private business

Acceptable at certain times

On-line gaming (educational)

On-line gaming (non educational)

On-line shopping / commerce

File sharing (eg Bit Torrent, Limewire)

Use of personal social networking sites (while "at work")

Use of an official group social networking site

Use of video broadcasting e.g. Youtube

How you use technology to communicate.

Personal Devices - An agreed policy is in place regarding the use of devices belonging to others. Some areas are signposted as “No Mobile” areas (eg toilets or changing rooms) while others are areas where people know they can use their mobiles freely and safely.   An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users

This is an area of rapidly developing technologies and uses. Groups will need to discuss and agree how they intend to implement and use these technologies. The table has been left blank for organisations / groups to choose their own responses. The following table shows how this group currently considers the benefit of using these technologies outweighs their risks / disadvantages:

Staff & volunteers, Young people, Communication Technologies

Allowed at certain times Allowed with staff / volunteers permission

- Use of online communication technologies eg social networking, chat rooms, instant messaging, email
- Use of hand held devices eg gaming consoles
- Use of the organisation's email for personal emails (limited, must make clear that author acting in personal capacity, not representing organisation).

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

The group'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 in accordance with the group's policy, 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.

Protecting professional identities

This section covers an area of professional concern that has become more relevant in recent years. The appendix to this document includes references to some important guidance – in particular the "Guidance for Safer Working Practice for Adults who work with Children and Young People"

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 the group
- not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including email, 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 the group 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 (wherever possible) take place using the group's official equipment / systems.

Any communications outside the agreed protocols (above) 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 the group. 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 what they find.(Research shows that many employers use such searches, but few employees / applicants for jobs realise this)

Social Networking sites are spaces that young people inhabit and yet many professionals overlook the potential they have, if well managed, to bring together young people and professionals, particularly young people that are hard to reach by traditional means. Groups are therefore beginning to develop official social networking sites for their group where young people and professionals can participate using online technologies with which they are familiar. This brings not only positives but also areas of concern that can leave an organisation or individual vulnerable. Further guidance is available from SWGfL for those organisations who wish to use such technologies.

Thank you to for draft templates www.onlinecompass.org.uk

Approved by the Chair, Reyaz Limalia on behalf of the Trustees September 19th 2017

to be reviewed on or before 30th September 2018

Reyaz Limalia