



Online Safety Policy

Signature		Les Mettrick	Date 14th March 2024
Signature		Lee Paxton	Date 14 th March 2024
Signature		Hayley Sykes	Date 14 th March 2024
Signature		Jackie Mc Gregor	Date 14th March 2024
Signature		Carl Hope	Date 14th March 2024

Contents

1. Aims.....	2
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	3
4. Educating young persons about online safety.....	5
5. Educating parents about online safety.....	6
6. Cyber-bullying.....	6
7. Acceptable use of the internet in centre.....	7
8. Young persons using mobile devices in centre.....	8
9. Staff using work devices outside centre.....	8
10. How the centre will respond to issues of misuse.....	8
11. Training.....	8
12. Monitoring arrangements.....	9
13. Links with other policies.....	9
Appendix 1: EYFS and KS1 acceptable use agreement (young persons and parents/carers) Error! Bookmark not defined.	
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (young persons and parents/carers).....	10
Appendix 3: acceptable use agreement (staff, trustees, volunteers and visitors).....	11
Appendix 4: online safety training needs – self audit for staff.....	12
Appendix 5: online safety incident report log.....	13

1. Aims

Our centre aims to:

- Have robust processes in place to ensure the online safety of young persons, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole centre community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for centres on:

- [Teaching online safety in centres](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for Directors and staff](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given trainers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on young persons' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trustee board

The Trustee board has overall responsibility for monitoring this policy and holding the Director to account for its implementation.

The trustee board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The trustee who oversees online safety is Hayley Sykes.

All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the centre's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some young persons with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Director

The Director is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the centre.

The Director is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure young persons are kept safe from potentially harmful and inappropriate content and contact online while at centre, including terrorist and extremist material
- Ensuring that the centre's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the centre's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the centre behaviour policy

This list is not intended to be exhaustive.

3.3 The Designated Safeguarding Lead

Details of the charities DSL (D.Lumb) is set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in centre, in particular:

- Supporting the Director in ensuring that staff understand this policy and that it is being implemented consistently throughout the centre
- Working with the Director and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the centre child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately.
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in centre to the Directors and/or trustee board

This list is not intended to be exhaustive.

3.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the centre's ICT systems and the internet (appendix 3), and ensuring that young persons follow the centre's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the centre behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.5 Parents

Parents are expected to:

- Notify a member of staff or the Directors of any concerns or queries regarding this policy
-

- › Ensure their child has read, understood and agreed to the terms on acceptable use of the centre's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- › What are the issues? – [UK Safer Internet Centre](#)
- › Hot topics – [Childnet International](#)
- › Parent resource sheet – [Childnet International](#)
- › Healthy relationships – [Disrespect Nobody](#)

3.6 Visitors and members of the community

Visitors and members of the community who use the centre's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating young persons about online safety

Young persons will have been taught about online safety as part of the curriculum at the school they attended.

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All SCHOOLS have to teach:

- › [Relationships education and health education](#) in primary centres
- › [Relationships and sex education and health education](#) in secondary centres

In **Key Stage 1**, young persons will be taught to:

- › Use technology safely and respectfully, keeping personal information private
- › Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Young persons in **Key Stage 2** will be taught to:

- › Use technology safely, respectfully and responsibly
- › Recognise acceptable and unacceptable behaviour
- › Identify a range of ways to report concerns about content and contact

By the **end of primary centre**, young persons will know:

- › That people sometimes behave differently online, including by pretending to be someone they are not
- › That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- › The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- › How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- › How information and data is shared and used online
- › What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- › How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, young persons will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Young persons in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary centre**, young persons will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Sunshine Sunflower Foundation will teach:

The safe use of social media and the internet and where necessary, teach about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some young persons with SEND.

5. Educating parents about online safety

The charity will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Directors and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Directors.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the centre behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that young persons understand what it is and what to do if they become aware of it happening to them or others. We will ensure that young persons know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The charity will actively discuss cyber-bullying with young persons, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Gardener are also encouraged to find opportunities to cover cyber-bullying.

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support young persons, as part of safeguarding training (see section 11 for more detail).

The charity also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying where illegal, inappropriate or harmful material has been spread among young persons, the charity will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Charity staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on young persons' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the centre rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of centre discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a young person discloses that they are being abused and that this abuse includes an online element.

Any searching of young persons will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The centre's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on young persons' electronic devices will be dealt with through the centre complaints procedure.

7. Acceptable use of the internet in centre

All young persons, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the centre's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the centre's terms on acceptable use if relevant.

Use of the centre's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by young persons, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Young persons using mobile devices

Young persons may bring mobile devices into charity, but are not permitted to use gardening

➤ Any use of mobile devices in centre by young persons must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a young person may trigger disciplinary action in line with the centre behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Director.

10. How the centre will respond to issues of misuse

Where a young person misuses ICT we will follow the procedures set out in our policies on ICT and Internet acceptable Policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The charity will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training every year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure young persons can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence young persons to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL (Debbie.Lumb) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL and chair of trustees. At every review, the policy will be shared with the trustee board. The review will be supported by an annual risk assessment that considers and reflects the risks young persons face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Young persons and parents/carers

ACCEPTABLE USE OF THE CENTRE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR YOUNG PERSONS AND PARENTS/CARERS

Name of young person:

I will read and follow the rules in the acceptable use agreement policy

When I use the ICT systems (like computers) and get onto the internet I will:

- Always use the ICT systems and the internet responsibly and for educational purposes only · Only use them when a trainer is present, or with a trainer's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my trainer or parent/carer
- Tell a trainer (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my trainer has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a trainer
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the centre's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device:

- I will not use it during sessions without a trainer's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the centre will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (young person):

Date:

Parent/carer's agreement: I agree that my child can use the centre's ICT systems and internet when appropriately supervised by a member of centre staff. I agree to the conditions set out above for young persons using ICT systems and internet, and for using personal electronic devices in centre, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 3: acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE CENTRE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS

Name of staff member/trustee/volunteer/visitor:

When using ICT systems and accessing the internet in centre, or outside centre on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the centre's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the centre's network
- Share my password with others or log in to the centre's network using someone else's details
- Take photographs of young persons without checking with trainers first
- Share confidential information about the charity, its young persons or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the centre

I will only use the ICT systems and access the internet in centre, or outside centre on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the charity will monitor the websites I visit and my use of ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside centre, and keep all data securely stored in accordance with this policy and the centre's data protection policy.

I will let the designated safeguarding lead (DSL) know if a young person informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the centre's ICT systems and internet responsibly and ensure that young persons in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety?	
Are you aware of the ways young persons can abuse their peers online?	
Do you know what you must do if a young person approaches you with a concern or issue?	
Are you familiar with the centre's acceptable use agreement for staff, volunteers, trustees and visitors?	
Are you familiar with the centre's acceptable use agreement for young persons and parents?	
Do you regularly change your password for accessing ICT systems?	
Are you familiar with the charities approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident