Sunbeams
Community Hub

A world in which Autism is celebrated.

Registered Charity No. 1152188

Employment

45. Social Networking Policy Including Online Safety

We recognise that the online world provides many positive opportunities, however it can present risks and challenges to children and young people.

We have a duty to ensure all children and young people in our organisation are safeguarded and protected from harm online. Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices.

Our online safety policy is consistent with our wider safeguarding policy.

It is the overall responsibility of the Designated Safeguarding Lead – Sue Carr for ensuring the safety of all children, young people, and adults within the organisation when online.

Policy

We expect all staff / volunteers to be professional and responsible when using social networks.

It is important that proper practice is followed when using the internet including social networking sites such as Facebook and Twitter. This is to protect the children/young people, /carers and staff in Sunbeams Play.

The Role of the Online Safety Lead

The Online Safety Lead – Sue Carr will:-

- ensure all staff/volunteers have current awareness of the online safety policy and incident reporting procedures.
- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies/procedures.
- offer advice and support to staff and volunteers.
- Complete training on online safety
- keep up to date with developments in online safety and cascades these to staff/volunteers.
- understand and know where to obtain additional support and where to report online safety issues.
- receive reports of online safety incidents and keeps a log of incidents to inform future online safety developments.
- communicate with parents/carers about online safety.
- monitor online incident logs

Staff/Volunteers

Staff members / Volunteers are allowed to use any social networking site as long as they follow these guidelines regarding the impact social networking has. Failure to comply with some guidelines may be an invasion of privacy and may infringe our confidentiality policy (1.4). These are also to guard your personal reputation and that of Sunbeams Play.

Staff and volunteers are given the Online Acceptable Use Agreement to sign during their induction. The Agreements sets out the standards which need to be adhered to when being online. (Appendix A)

The guidelines include but are not limited to:

- Staff / volunteers must not publicly mention any of the children / young people or families from Sunbeams Play on their online profiles.
- Staff / volunteers must avoid writing indirect suggestive comments about Sunbeams Play on their social networking sites e.g. “I’ve had a bad day at work”.
- Staff / volunteers must not publish photos of the children/young people on their online profiles.
- Staff / volunteers must not publicly write anything negative or inappropriate about other staff members / volunteers on their social networking sites.
- Staff / volunteers must not use their mobile phones to take photos or go on social networking sites whilst at work
- Staff / volunteers, children and young people will not be permitted to use their personal mobile phones or tablets whilst at Sunbeams Play, all mobile phones or devices are to be kept in personal lockers in the foyer, either turned off or on silent.
- In an emergency staff / volunteers may receive / make calls using the office landline, this should be agreed beforehand with the session leader for that day.
- Staff / volunteers must not mention Sunbeams Play inappropriately on their profiles.
- Staff / volunteers should consider the reputation of Sunbeams Play when posting a status, particularly prior to going to work. Remember we are caring for children/young people.
- Any derogatory comments made on social networking sites by staff / volunteers / parents or carers will be addressed by the manager. Parents / carers will be spoken to by the manager to resolve the situation. Staff / volunteers will also be spoken to by the manager and this could result in disciplinary procedures.
- In order to maintain professional boundaries staff / volunteers should not accept personal invitations to be friends from parents / carers / children / young people that use Sunbeams Play, unless they know them in a personal capacity.

Staff members / volunteers are advised to set their online profiles as private so that only friends are able to see their information. This can help to prevent any accidental breaches of this policy.

Please be aware that any serious breaches of this policy could result in disciplinary action.

Parents/carers

We respectfully ask that if parents/carers have any questions or queries regarding Sunbeams Play that they contact management through Sunbeams Play’s social media page and not individual staff pages.

Measures we have in our organisation to promote online safety.

- We have the following measures in place to promote online safety:
- A firewall and robust antivirus software
- A recognised internet service provider- BT
- Technical IT support is sourced via Netmatters who provide the latest operating system and security updates and a password protected Wi-Fi network
- Website content can only be added by Manager and Safeguarding Lead Sue Carr who also monitors Sunbeams social media pages.
- Posts on social media sites are vetted prior to being allowed and all comments are monitored through the day. Anyone thought to be a risk are removed and blocked.
- Sunbeams do not use handheld devices within the groups
- Children and young people are supervised at all times when using the password protected educational touch screen.
- Access to online content in the organisation is only available to managerial staff.
- Any removable media containing personal or sensitive data (e.g. USB sticks or devices that leave our organisation) are secured through password and/or encryption
- Personal data is managed in compliance with The Data Protection Act 2018 (GDPR) & the Data (use and Access) Act 2025
- Children are not permitted to bring in their own devices from home
- Passcode and lock screened are used on all devices
- Staff and volunteers are not permitted to use any devices in the organisation for personal use.
- All staff and volunteers are provided with Cyber security and E-Safety training
- Online safety information and awareness is provided to parents to increase their awareness of online safety risks and issues to children at home. This is done through:
  -meetings with parents
  -providing links to relevant good practice information/websites

Digital Images and Videos

We gain written permission from parents to record and use digital images and video of their children. Through this process, we respect their rights under the Data Protection Act 2018.

Parent's are asked to sign a declaration which sets out how we are able to use digital images/videos of their child taken by us while in Sunbeams care (Appendix B)

Our organisation removes most images once used those that are kept for promotional use are stored securely by transferring them to our secure Cloud account meeting legal requirements on how long we retain those images.

We share images with parents through secure routes that include parental sites such as Tapestry.

Online Communications

Our organisation uses a range of online services to communicate which include:

- Website
- Social media pages
- Social media messaging
- Text messaging
- Online portal pages (Tapestry)
- Email

All communications take place through clear and established systems and will be professional in nature.

Communications are monitored for concerns/complaints. There are processes in place to respond and resolve complaints or comments concerning our organisation or staff/volunteers.

All staff/volunteers will be asked to read and sign the Online Acceptable Use Agreement, which sets out rules on the use of personal online communications.

Platforms for Online Abuse and Types of Abuse

Online abuse can happen anywhere online that allows digital communication, such as: social networks, text messages and messaging apps, email and private messaging, online chats, online gaming, and live streaming sites.

Children may experience several types of abuse online:

- Bullying/cyberbullying
- Emotional abuse-which can include emotional blackmail
- Sexting-pressure or coercion to create sexual images
- Sexual abuse
- Sexual exploitation
- Grooming-perpetrators may use online platforms to build a trusting relationship with the child to abuse them

National Guidance and Legislation on Online Safety

The Online Safety Act 2023

The Act makes companies that operate a wide range of popular online services legally responsible for keeping people, especially children, safe online. Services must do this by assessing and managing safety risks arising from content and conduct on their sites and apps. The Law is based on 3 fundamental duties:

- protecting children;
- shielding the public from illegal content;
- and helping adult users avoid harmful – but not illegal – content on the biggest platforms.

Protecting Children

There are 2 categories of harmful content to children that tech firms must deal with.

- The first is “primary priority content”, such as pornography and the promotion of suicide and eating disorders (below the threshold of criminality). If sites allow such content, children must be prevented from encountering it and the Act expects age-checking measures to be used for this.

- The second is “priority content” such as bullying and posts that encourage children to take part in dangerous stunts or challenges. Children in age groups judged to be at harm from such content– must be protected from encountering this kind of material.

Ofcom have said that the new laws will roll out in three phases as follows, with the timing driven by the requirements of the Act and relevant secondary legislation: Phase one: Illegal content, Phase two: Child safety, pornography, and protecting women and girls, Phase three: Additional duties for categorised services.

The Data Protection Act 2018 (GDPR) & the Data (use and Access) Act 2025

To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. This legislation also applies to all electronic and online data.

Keeping Children Safe in Education 2023

This outlines the responsibilities that schools and colleges have in safeguarding children, including a requirement to ensure appropriate levels of online filtering and monitoring are in place-refer to pages 35-38.

Personal Mobile Phones and Smart Watches

There are safeguarding risks associated with the use of personal mobile phones and smart watches. Our organisation has measures in place to protect children from the unacceptable use of technology or exposure to inappropriate materials on this technology. It is the responsibility of all members of staff to be vigilant and to report any concerns.

Parents are asked to keep all phones and mobile technology at home, however if they are brought into the center it is made clear that all:

Personal mobile phones are:

- To be stored securely in the lockers provided.
- Only to be used in the staffroom
- To be stored on silent mode
- Not to be used to conduct any work for the organisation
- Not allowed to connect to the Wi-Fi at any time

Smart Watches

- Only smart watches without cameras are permitted to be worn when working with children.
- Watches with cameras will need to be removed before work and stored securely in the lockers provided.
- The following steps must be adhered to by staff wearing smart watches without cameras:
- Smart watches are not allowed to connect to the organisations Wi-Fi at any time
- To ensure there is no internet or Wi-Fi connection all other functions must be disabled with Bluetooth disconnected or on 'flight mode',
- The watch must be on silent at all times
- Staff must not use their smart watch to access photos or images while working
- Staff need to be vigilant of others checking their smart watches and remind them of our policy
- With ongoing technology advances, the organisation reserves the rights to request the removal of a Smart Watch if it deemed a safeguarding risk to children.

Responding to online abuse and how to report it

The Online Safety Lead (Sue Carr) should be used as a first point of contact for concerns and queries on online abuse. All concerns about a child should be reported to them without delay and recorded in writing using the agreed system as set out in the safeguarding policy.

Following receipt of any information raising concern about online abuse, the Online Safety Lead will consider what action to take and seek advice from the Norfolk Children's Advice & Duty Service (CADS) as required.

If, at any point, there is a risk of immediate serious harm to a child, The Children's Advice and Duty Service (CADS) should be contacted. Anybody can contact CADS in these circumstances. Depending on the type of online abuse concerned, this will also be reported using the relevant method below:

- **Criminal Sexual Content-**If the concern is about online criminal sexual content, this will be report to the Internet Watch Foundation report.iwf.org.uk/en/report
- **Child Exploitation and Online Protection**- If the concern is about online sexual abuse and grooming, a report should also be made to the Child Exploitation and Online Protection (CEOP) www.ceop.police.uk/safety-centre/

- **Report Remove Tool**-Young people under 18 will be supported to use the Report Remove tool from Childline to confidentially report sexual images and videos of themselves and ask these to be removed from the internet. This can be reported at www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/
- **Online Terrorism or Extremism Content-**If online material is found which promotes terrorism or extremism this will be reported to ACT Action Against Terrorism. A report can be made online at act.campaign.gov.uk/
- **Online Hate Content**-If online content incites hatred this will be reported online to True Vision www.report-it.org.uk/your_police_force

This policy was adopted on	20th April 2015
Policy updated	April 2026
Next review date	April 2027

Signed on behalf of the management committee

Name of Signatory - Susan Carr

Role of Signatory - CEO

Reviewed By	Date
Sue Carr	24/04/2024
Sue Carr	16/05/2025
Sue Carr	28/04/2026

Appendix A

Online Acceptable Use Agreement for Staff and Volunteers

New technologies have become integral to the lives of children and young people in today's society, both within schools and settings and in their lives outside of schools and settings.

The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Agreement is intended to ensure:

• that staff and volunteers will be safe and responsible users of the internet and other digital technologies
• that Sunbeams and users are protected from accidental or deliberate misuse.

Sunbeams will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities and activities for service users and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use Sunbeams ICT in a responsible way, to minimise the risk to my safety or to the safety and security of Sunbeams and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

• I understand that Sunbeams will monitor my use of its ICT systems including any email and other digital communications technologies.

This may include but not be limited to the following circumstances:

o When staff leave or are on long-term absence for retrieval or redirection of messages.

o When a member of staff is under investigation or suspected of illegal, fraudulent, inappropriate or safeguarding activity.

o To collect and review information contained in any electronic system for documented purposes, for example, to complete a Subject Access Request or similar.

• I understand that information and resources stored on the organisations equipment and drives should be considered to be controlled and accessible by the Sunbeams and authorised staff.
• I understand that this agreement also apply to use of Sunbeams systems out of Sunbeams (eg laptops, email, Tapestry etc). This includes my personal or work mobile phone or tablet if it contains my work email.

• I understand that the Sunbeams systems are primarily intended for support for vulnerable people within our community and that I will only use the systems for personal or recreational use within the policies and rules set down by Sunbeams.

• I will keep my usernames and passwords private and will not try to use anyone else's username and password.

• I will return all Sunbeams owned ICT equipment and delete all Sunbeams data from my personal devices when I leave my employment.

• I will immediately report any illegal, inappropriate or harmful material or incident, to the Centre Manager or other person appointed by the Center Manager/Trustees

I will be professional in my communications and actions when using school ICT systems:

• I will not access, copy, delete or otherwise alter any other staff members files, without their permission.

• I will communicate with others in a professional manner.

• I will ensure that when I take or publish images of service users or parents/colleagues, I will do so with their permission and in accordance with the Sunbeams's Agreement. I will not use my personal equipment to record these images, unless I have permission to do so.

• Where these images are published (eg on Sunbeams website / facebook) it will not be possible to identify service users by name, or other personal information.

• I will not use chat and social networking sites whilst in Sunbeams, unless it relates to Sunbeams facebook page.

• I will only communicate with service users and parents / carers using official Sunbeams systems and in a professional manner. I will not share any personal information with a service user (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.

• I will not engage in any on-line activity that may compromise my professional responsibilities.

• I will lock my screen or log off my computer should I leave it unattended. • I will not allow a third party to access my work emails on my mobile phone or tablet

Sunbeams have the responsibility to provide safe and secure access to technologies:

• When I use my personal handheld / external devices in Sunbeams (PDAs / laptops / mobile phones / USB devices etc), I will follow the rules set out in this agreement, in the same way as if I was using Sunbeams equipment. I will also follow any additional rules set by Sunbeams about such use. As far as I am able, I will ensure that when connecting these devices to Sunbeams ICT systems, they are using up to date Operating Systems (e.g. latest versions of Android / iOS) and protected buy up-to-date anti-virus software where applicable.

• I will encrypt (Password Protect in most cases) my personal device if I use it to access Sunbeams personal data.

• I will inform the Sunbeams' Manager or other person appointed by the Manager if my personal device e.g. phone or tablet is lost or stolen should it contain any of Sunbeams personal data.

• I will immediately report any Internet content that is not filtered that I suspect could be inappropriate.

• I will not use personal email addresses for work-related purpose.

• I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

• I will ensure that my data is regularly backed up

• I will not upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (eg child sexual abuse images, criminally racist material, adult pornography etc).

• I will not use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.

• I will not install or attempt to install programmes of any type, nor will alter computer settings, unless this has been authorized by the Manager.

• I will not disable or cause any damage to Sunbeams equipment, or the equipment belonging to others.

• I will only transport, hold, disclose or share personal information about myself or others, as outlined in Sunbeams Data Protection Policy.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for Sunbeams sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work.

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

• I understand that this Acceptable Use Agreement applies not only to my work and use of Sunbeams equipment the centre, but also applies to my use of Sunbeams systems and equipment out of Sunbeams centre and my use of personal equipment in Sunbeams or in situations related to my employment by Sunbeams.

• I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use Sunbeams in and out of Sunbeams and my own devices (in Sunbeams and when carrying out communications related to Sunbeams) within these guidelines.

Signed: …….. Print name: …….

Date: …….

Appendix B

Data Protection Permissions Slip

I …… Parent/Carer of ……..……
Confirm that I am happy for Sunbeams to hold information about myself and my child(ren) and am aware that this includes paper records locked away securely. Journals recording my child(ren) whilst attending Sunbeams and on the Sunbeams Cloud, which allows secure access to information to the Management team and Senior Trustees.

Signed:…… Name (Print): …….. Date: …….

I also give permission to be contacted by email with information from Sunbeams including newsletters and any other information regarding outings etc.

My email address is: …….

Signed:…… Name (Print): …….. Date: …….

I/we are happy for Sunbeams to use my child(ren)s/young persons photo as agreed below:

Child/young persons Journal	☐
Other children/young peoples Journals	☐
Facebook	☐
Twitter	☐
Sunbeams website	☐
Promotional Material	☐
Newspapers	☐
Posters	☐

I understand I can add or withdraw permission at any time in the future.

Signature: …… Print name: …… Date: ……..