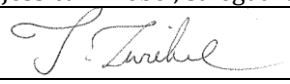
Sunbeams

DIGITAL SAFEGUARDING, IT, AND INTERNET POLICY

Document Control Sheet

Document Title	Sunbeams Digital Safeguarding, IT and Internet Policy
Document Reference	SBP3
Version Number	13
Date Created	September 2015
Date Approved	September, 2025
Next Review Date	September, 2026
Status	Approved
Approved By	Jessica Zwiebel, Safeguarding Officer and Trustee
Signature	

Revision History

Version	Date	Author	Description of Change	Approved By
1.0	Sep 2015	Safeguarding Lead	Initial draft outlining acceptable use of computers and email for staff.	Board of Trustees
2.0	Dec 2015	Safeguarding Lead	Introduced e-safety section following youth feedback on online risks.	Board of Trustees
3.0	Sep 2016	Safeguarding Lead	Review	Board of Trustees
4.0	May 2018	Safeguarding Lead	Major revision for GDPR compliance; privacy and consent clauses added.	Board of Trustees
5.0	Apr 2019	Safeguarding Lead	Review	Board of Trustees
6.0	Mar 2020	CEO and Safeguarding Lead	Added remote-working guidance and online communication procedures during COVID-19.	Board of Trustees
7.0	Mar 2021	Safeguarding Lead	Review	Board of Trustees
8.0	Mar 2022	Safeguarding Lead	Review	Board of Trustees
9.0	Jul 2022	Administrator	Refreshed formatting and aligned with staff code of conduct.	Board of Trustees
10.0	Jul 2023	Safeguarding Lead	Review	Board of Trustees
11.0	Jul 2024	Safeguarding Lead	Review with Interlink staff.	Board of Trustees
12.0	May 2024	Administrator and Safeguarding Lead	Merged IT and Internet Use with Digital Safeguarding Policy; full reformat.	Board of Trustees
13.0	Oct 2025	Safeguarding Lead	Comprehensive annual review; aligned with LY Quality Mark (Bronze) standards.	Board of Trustees

1. Policy Statement

Sunbeams London Ltd does not permit any young person to access the internet or online platforms on-site or via organisational devices. Internet access is restricted to staff and, occasionally, to volunteers, and is strictly monitored and filtered using the TAG (Technology Awareness Group) system to ensure safety and alignment with our safeguarding principles and Orthodox Jewish ethos.

Where limited digital content (e.g. short video clips) is used as part of a mentoring interaction, this is done:

-only with prior approval by a Project Coordinator,
-only using vetted content, and
-only with parental written consent on a case-by-case basis.

All staff and volunteers are required to follow safeguarding guidance regarding digital content and must never share internet-enabled devices with mentees.

Sunbeams restricts all digital and internet communication to internal operational use only. Service users (girls, parents, or families) do not have access to online communication on the premises, and no member of staff or volunteer may contact a service user via digital or online means. All permitted digital activity must support Sunbeams' operational, administrative, or safeguarding functions, take place through secure, approved systems, and comply with the Data Protection Policy and Code of Conduct.

2. General Principles

Sunbeams London Ltd recognises the benefits that email, and internet use offer and access to both will be given to all staff and volunteers who use a computer in the course of their work and have been allocated a personal password.

Sunbeams is also aware of the potential risks involved with such technology and it is our aim to protect anyone from danger by providing as safe an environment as possible.

Employees will be provided with an internet connection and allocated an email account with an address for research purposes and work-related communications. Passwords will be allocated by the office Manager at an early stage in the induction process.

You are responsible for the security of your terminal; access must not be allowed to unauthorised persons and passwords must not be divulged to anyone, even colleagues.

All queries regarding this policy, regarding security matters, access to software and possible breaches of the policy should be directed to the office manager, Mrs Ruchi Ostreicher, who will bring it to the attention of the Mrs Yocheved Zwiebel, the director.

All internal digital communication must reflect the same professionalism and confidentiality expected in all Sunbeams work. Humour, slang, or personal comments should be avoided on official systems. Discussions about children or families take place only within authorised, confidential channels.

Only staff and authorised volunteers may access the internet on Sunbeams' filtered and monitored systems. Any external link, platform, or file-sharing tool must be approved by the Office Manager and comply with Sunbeams' data security protocols.

3. Email

The advantages of using email include:
-It is a fast and inexpensive way of delivering messages and documents over long or short distances.
-Information can be shared quickly and consistently between any number of people. It removes the need to print and distribute information by conventional means.
-However, there are a few challenges associated with e-mail and employees should note the following:

E-mail is not the informal and transient form of communication that many people think it is, even 'deleting' or 'trashing' a message does not mean it is unrecoverable, and it has the same authority as any other communication to and from the organisation. Binding contracts may be inadvertently created.

The same laws apply to email as to any other written document and therefore employees should avoid making any inaccurate or defamatory statements about colleagues or other parties (deliberate or otherwise).

E-mails are not confidential and can be read by anyone given sufficient levels of expertise.

The ease and speed of e-mail can lead to inadequate thought going into a message, and the possibility of the words or tone being misinterpreted by the recipient. Abrupt, inappropriate and unthinking use of language can lead to a bullying tone and possible offence to others even harassment, for example, capitals are often interpreted as shouting.

It can stifle face to face communication or be used to abdicate the responsibility of communicating messages that should be done in person. Consider whether a phone call may be a better way of discussing a complex or confidential matter.

Intensive use of e-mail, and unnecessarily wide broadcasting, can lead to 'information overload' with vital information being lost in many messages that are irrelevant and risking stress as colleagues try to keep up with the number of e-mails received.

A disclaimer will be added automatically to external email, but employees must act responsibly when writing email and seek advice from their line manager before sending a message if there is any doubt about its contents. Wrongly delivered messages should be redirected to the correct person.

If the email message contains confidential information, no use should be made of that information, nor must it be shared. The importation of viruses is often through downloading files and programmes from external sources.

4. Internet

The internet can be an invaluable tool or resource to support employees' normal duties and responsibilities and gives access to large amounts of information which is often more up to date than in traditional sources like libraries. Unfortunately, as the internet is uncontrolled, some of this information is less accurate than it may appear. Employees should be aware that there are risks attached to obtaining and using such unregulated information.

Employees are expected to use the internet only for work purposes during worktime. Researching on the web can be time consuming and it is very easy to become unfocused when browsing. However, they may, in their own time and only during office hours, use Sunbeam's internet for their own purposes (such as shopping), subject to sites being in keeping with Orthodox Jewish ethos.

5. Data Protection and Record Keeping

All staff must handle personal and sensitive data in accordance with the Data Protection Act 2018 and UK GDPR.
Work files must be stored only on approved, secure drives with restricted access.
Personal devices must not store Sunbeams data unless encrypted and authorised.
Emails containing personal information must be password-protected, with passwords shared separately.
When data is no longer required, it must be securely deleted or destroyed following the retention schedule.

6. Introduction of Viruses

The greatest risk from viruses lies in downloaded programs and executable files. All software for use in this organisation must be obtained from legal sources controlled by the office manager. Software may not be downloaded without the office manager's clearance.

7.Watching videos

There may be occasions when mentors would like to show a video, or video clip, or other device for sharing images as a treat for a mentee. They will be required to seek authorisation on a case-by-case basis. Several conditions will need to be satisfied.
The project co-ordinator will need to authorise the activity.

The video selected will need to have the content vetted.
-Parental written consent will to be sought for each occasion.
-It should be short and as a guide, approximately 15 minutes.
-It should never be more frequent than once per month and preferably no more than four times per year.

However, employees must note that any breaches of the rules for access noted under 'Misuse' below will be dealt with under the organisation's disciplinary procedures and will be treated very seriously.

8. Filtering System

Filtering software will be used to protect against misuse of the internet in our workplace.

Filtering software may on occasions eliminate material that is acceptable. Sunbeams is willing to consider releasing such sites on request, but only after carefully checking its content. Portals are pass-worded and can only be altered with consent from the Office Manager and Mr Geller (IT technician), the password holders.

Conversely filtering software might on occasions fail to eliminate unacceptable material. Sunbeams cannot accept liability for any distress caused in this way.

Where unsuitable sites are discovered the web address must be reported immediately to an IT technician so that the filtering software can be manually updated.

9. Monitoring

Employees and volunteers should be aware that Sunbeams reserves the right to monitor internet site visits and all type of network activity by employees or volunteers. Sunbeams strongly discourage sending and receiving personal emails through the organisation's domain and cannot promise privacy for such activity.

10. Misuse

Employees and volunteers should note that the following list of possible areas of misuse is not exhaustive and that some are illegal

-Intentionally seeking to damage or disrupt any part of the IT facilities or breaching the IT security controls
-Deliberate accessing of offensive, obscene or indecent material from the internet, such as pornography, racist or sexist material, violent images, incitement to criminal behaviour etc is forbidden.
-Accessing online diaries, known as web logging or 'blogging' is unacceptable use. This organisation should not be discussed on an online diary or on messenger boards.
-The sending of inappropriate messages, for instance, any message that might cause offence or harassment on grounds of the protected characteristics under the 2010 - Equality Act is forbidden.
-Copyright and licensing restrictions might apply to downloaded and forwarded material, whether internet or e-mail, including unauthorized software, games, and magazine disc items etc.
- Uploading any personal, sensitive, or confidential data about service users, staff, or volunteers into third-party AI tools or external platforms.
-Using AI for any task involving personal data without prior DPO approval.

Only anonymised, administrative tasks (e.g., formatting or scheduling) may be supported by AI, subject to DPO approval. All AI outputs must be reviewed for accuracy and bias before use.

Employees and volunteers should note that sites visited via the internet are traceable.

11. Breach of Policy (Discipline)

Employers carry a high degree of responsibility for their employees' activities when using e-technology. Because of this responsibility, misuse of the organisation's email or internet facilities will be treated very seriously.

Unacceptable behavior, such as harassment, bullying, offensive remarks or comments of a racial or sectarian nature, or regarding sexual orientation or relating to any of the other protected characteristics under the 2010 Equality Act, is just as serious an offence if committed during using ICT facilities as at any other time and will not be tolerated.

Breaches of policy or misuse will be dealt with under the organisation's disciplinary procedures. Such breaches could range from being inconsiderate to illegal activity; therefore, action taken under these procedures could range from a verbal warning to instant dismissal.

All digital or data-related concerns — such as accidental data sharing, system breaches, or exposure to harmful material — must be reported immediately to the Designated Safeguarding Officer (DSO) or Data Protection Officer (DPO).
Incidents are recorded using the Digital Incident Form and reviewed to identify learning and improvements.
Where applicable, serious data breaches are reported to the Information Commissioner's Office (ICO) within 72 hours.

12. Online Safety Oversight

The designated Online Safety Lead is Mrs Ruchi Ostreicher (Office Manager). Any issues related to digital safety, filtering concerns, or inappropriate content must be reported directly to her. Oversight of this policy, including updates and incident response, is managed jointly with the Designated Safeguarding Lead.

All staff receive induction and periodic training on safe digital practice. Antivirus, device encryption, and software updates must remain active on all systems. Lost or stolen devices must be reported immediately to the Office Manager and DPO.

13. Young People and Online Safety

Although Sunbeams does not provide internet access to children and young people on its premises, we recognise that our service users may be active online in their home and school environments. It is therefore essential that our staff and volunteers remain alert to online risks and know how to respond appropriately.

The main online risks for children and young people include:

- Cyberbullying – bullying or harassment using digital devices, messages or social media.
- Online grooming – when someone builds a relationship with a young person online in order to exploit or abuse them.
- Sexting/Sharing of images – when young people are pressured to share sexual messages or pictures.
- Radicalisation – exposure to extremist content online that could influence behaviour

or beliefs.
- Harmful content – exposure to violence, pornography, or other age-inappropriate material.

14. Social Media

social media may not be accessed at work and, whilst Sunbeams cannot restrict staff or volunteers outside of the organisation, employees and volunteers should be mindful that using mediums such as Facebook and twitter and posting statements about work, or offensive images of staff that can be viewed by wider community members is an offence and can bring Sunbeams into disrepute.

If staff or volunteers use social media accounts and bring Sunbeams into disrepute through any inappropriate images or statements, this behaviour will result in disciplinary action.

Staff and volunteers must remain vigilant to these risks and raise any concerns immediately, following the reporting process in the Sunbeams Safeguarding Policy. Any disclosures or incidents relating to online activity must be recorded using the Safeguarding Disclosure Form.

Sunbeams are committed to supporting parents to manage digital safety in culturally appropriate ways. Staff will, where helpful, signpost families to trusted resources such as the NSPCC, CEOP (Child Exploitation and Online Protection Centre), and the Technology Awareness Group (TAG).

By embedding online safety within our safeguarding practice, Sunbeams ensures that digital risks are taken seriously and that children and families are supported to remain safe in all contexts.

Trustees: Ensure this policy is implemented and adequately resourced.
Designated Safeguarding Officer (DSO): Oversees digital safety, reporting, and safeguarding compliance.
Office Manager: Monitors staff use of digital systems and filtering compliance.
All Staff and Volunteers: Follow this policy, use digital systems responsibly, and report any concerns promptly.