GS10 – Green Synergy IT Management and Security Policy

Purpose of the Policy
Green Synergy is committed to ensuring that the charity's policy framework is inclusive, responsive, robust and accountable. The organisation believes that sound policies are required in the defining the policy and procedures the charity will operate and abide by when managing information technology security. This will significantly benefit the overall efficiency of the operations for Green Synergy and promote the best interests of its service users, employees, volunteers, Trustees, participants, partners / stakeholders and voluntary officers.

Statement of Policy – Green Synergy provides its employees with access to IT, email, internet system, cloud hosted drives and social networking sites and its use is encouraged where such use is suitable for business purposes and support the goals and objectives of the charity. Green Synergy's electronic devices are interconnected on a network that spans the whole charity and enables information to be shared amongst users. It is possible for problems to be caused by individuals using the Green Synergy computer system for inappropriate or non-business purposes (e.g. non-authorised used of mobile devices, downloading material from the internet or copying files from personal disks or USB's) which may compromise the security of data and operation of systems.

Policy Principles – Green Synergy IT Management and Security Policy aims to:

- Ensure that Green Synergy's computer systems and network are used and secured properly and that users understand what is expected of them.
- Reduce problems such as the interruption of computer services that could affect our work.
- Help prevent legal and regulatory problems.

This policy should be read in conjunction with the charity's Safeguarding Policies and Data Protection Policy.

Scope of Policy - This Policy applies to all employees and contractors of Green Synergy and subsidiaries, including freelancers and temporary staff. All staff, contractors and volunteers are required to familiarise themselves with this policy and sign up to comply with it to ensure that computer systems are protected from external threats such as viruses and hacking.

IT Management and Security Policy

1. **Security and Administration of the System**
   a. All central computer systems, environments and information contained within them will be protected against unauthorised access by tight controls on administrator

Green Synergy. 49 Roman Pavement, Lincoln, Lincolnshire. LN2 5RD. Tel: 01522 533077
Charity Number: 1153883 Company Number: 08399741
Email: info@greensynergy.org.uk Web: www.greensynergy.org.uk

access (restricted to our IT support company and administrators JSM Computers), secure login and appropriate access limitations.

b. Information kept on these systems will be managed securely, to comply with relevant data protection laws. All personal information will be password protected. See our GS7 Green Synergy Data Protection Policy.

c. Line managers have a responsibility for ensuring the implementation of adherence to and compliance with this policy throughout their areas of functional responsibility.

d. The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of everyone.

e. All users have a responsibility to report promptly any incidents which may have an IT security implication for Green Synergy. All breaches of security must be reported to the Chief Executive.

f. Green Synergy protects against loss of systems and data by ensuring that our systems are regularly maintained by external IT Support provided by JSM Computers. This includes regular examination of our boundary firewalls, access control, patch management, password-based authentication, anti-malware software and security of internet connection.

g. The Senior Management Team will devise a cybersecurity incident response plan and explore Cyber Essentials accreditation for the charity.

2. Logins and Passwords

a. Individuals are responsible for their own login IDs and passwords. These should only be used for work purposes and should never be disclosed to third parties (including colleagues). Disclosure to a third party means the authorised user could be held responsible for actions taken by the other party on the system. NEVER use someone else's log in.

b. Individuals should ensure that passwords are changed at regular intervals. Green Synergy's system through Microsoft should automatically prompt you to change your email once every 2 months.

3. **Corporate Image and Reputation**

a. Messages sent via Green Synergy's email, internet system and social networking sites, especially those to young people, must be written in accordance with the standards of any other form of written communication and the content and language used in the message must be consistent with Green Synergy practice.

b. Green Synergy staff must ensure that they do not create unnecessary business risk to the charity or its reputation by their misuse of the internet. The distribution of any

information about Green Synergy through the internet, through social networking, computer-based services, email and messaging systems is subject to the scrutiny of the charity. Green Synergy reserves the right to determine the suitability of this information.

4. Firewalls and Viruses

a. Any attempt to intentionally introduce a virus will be viewed as Gross Misconduct that will lead to dismissal, as will any attempt to harm Green Synergy's, or others', computer systems.

5. Use of Mobile Devices

a. Staff (especially freelance staff) may need a mobile device for work. If they do this device should be signed out and signed back. We will ensure that the device has the right level of security for use.

b. Staff and volunteers may use their own computer systems and mobile devices to access email, work social media and documents if this has been authorised and logged with the Finance and Office Manager. Staff must ensure that their computer or mobile device complies with Green Synergy's IT policy and that they only use secure apps rather than web browsers to access information.

6. Monitoring

a. Green Synergy accepts that use for the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and reputation of the charity. Therefore, the charity reserves the right to monitor any information on Green Synergy's computer systems, including email and internet usage. Green Synergy will not carry out any targeted monitoring of an individual unless there is evidence of abuse. Any such targeted monitoring will require the prior approval of the Chief Executive.

7. Inappropriate Material

a. It is prohibited to send, receive, browse, download, copy or print any material that is abusive, defamatory, obscene, sexually explicit, racist, pornographic, sexist, homophobic, untrue, malicious or offensive, or that might harass or intimidate another person or that breaches copyright. The downloading, transmitting, accessing or acquiring of such materials will be treated as Gross Misconduct, which can result in employee dismissal.

8. **Privac**y

a. It is illegal under the Data Protection Act 1998 (the 1998 Act), the 2018 Act, any subsequent amendments and the General Data Protection Regulation (GDPR) 2018 to

disclose someone else's personal details without their permission. In some circumstances (particularly re: child protection it may be necessary to share personal details. Refer to our Safeguarding Policies for more guidance).

b. Employees should also take care when revealing their own personal details over the internet or by email. The transmission of personal data through electronic communications systems is inherently risky.

9. Policy on the use of Green Synergy computers

a. You should not use Green Synergy computers/ mobile devices:
   i. to install any software, whether on a disk/USB or from the Internet (this includes games, screen savers, custom cursors, etc.). If upgrades need to be made to software, make the Finance and Office Manager aware ahead of time.
   ii. to forward confidential information from third parties or personal information without the appropriate authorisation being obtained.

b. You should not attempt under any circumstances to bypass or modify any Green Synergy security mechanisms, virus protection systems or other software. Attempting to bypass the settings may put you or your user account at risk.

c. You should not make copies of any Charity-owned software nor distribute copies of any Charity-owned software.

d. Employees (both permanent staff and freelance workers/ sessional staff) using Green Synergy owned hardware outside Green Synergy premises (e.g. working at home or offsite) are responsible for the safety and maintenance of the equipment in question and the data stored thereon or on charity systems accessed remotely. Computers need to be opened up and linked to the internet once a week to get their virus and Microsoft updates. If this is not done and the computer gets a virus, the member of staff will be liable for the costs of repair.

e. Green Synergy owned computers should not be used for anything others than work purposes unless authorised to do so by their line manager and IT admin. Freelance computers will be logged back into the system and wiped of information and documents at the end of each project.

f. Green Synergy staff, volunteers and freelancers/sessional staff must:
   i. Always check files brought in on removable media (such as CD's, DVD's, USB keys...) with antivirus software and only use them if they are found to be clear of viruses.

ii. Protect the computers from spillages by eating or drinking well away from Green Synergy owned IT equipment.
iii. Contact the IT provider if they are want to use a currently unsupported machine. These machines are not to be used without up-to-date software and virus updates.

10. Email Policy

a. The charity's email should not be used:
   i. to send messages that are unrelated to the business activities of Green Synergy (subject to minimal personal use, as set out below)
   ii. to send or receive messages that are defamatory, racist, pornographic, sexist, homophobic or offensive or that might harass or intimidate another person.
   iii. to send attachments that are programmes capable of being run on another computer, such as games.
   iv. to instigate a mass sending of unsolicited email (ie. Spamming)
   v. to distribute works that are copyright protected.
   vi. to solicit e-mails that are unrelated to business activities or for personal gain.

b. Only open attachments to emails or click on links in them if they come from a trusted source. Attachments and links can contain or give access to malware (viruses or other programmes that could destroy files and software)

c. Phishing: Be alert to the risk of phishing. Phishing emails are disguised so that they appear to come from a trusted source but may ask for sensitive information such as bank details or encourage people to visit a fake website or open an attachment or link that contains or gives access to malware. If in any doubt, do not open the email or attachments.

d. Minimal personal usage of charity computers is permissible. However, such usage should be kept to a minimum and not allowed to interfere with work. Users are forbidden from using Green Synergy system to conduct private business activities.

e. An email message should be treated in the same way as a signed, handwritten letter on charity-headed stationery. As such your words and attached documents should be chosen carefully. It should be remembered that once an email has been sent it could be forwarded to others.

f. All outgoing email must bear the Green Synergy disclaimer, which currently reads:
   i. "This email is confidential and intended solely for the use of the individual to whom it is addresses. If you are not the intended recipient,

be advised that you have received this email in error and that any use, dissemination, forwarding, printing or copying of the email is strictly prohibited. Although this email and any attachments are believed to be free of any virus or any other defect which might affect any computer or IT system Into which they are received and opened, it is the responsibility of the recipient to ensure that they are virus free, and no responsibility is accepted by Green Synergy for any loss or damage arising in any way from receipt or use thereof. Green Synergy operates spam filters, and it is therefore possible that your emails sent to us may be blocked and deleted if they contain certain words and phrases that trigger the spam filtering software. If you have sent us an email requiring action and have not received a response, please telephone the intended recipient"

g. Employees must not send confidential information externally by email without the express authority of their line manager.

11. Internet Policy

a. Internet facilities on Green Synergy computers must not be used:

i. Visit Internet sites that contain obscene, hateful, pornographic or other illegal material except where you are expressly required to do so in the course of your work. In your role it is most unlikely that you will be required to access such material. In all circumstances access to illegal content is not allowed.

ii. to create, post or send any material containing pornographic, defamatory, racist, inaccurate or offensive content or material that breaches others' copyright

iii. to create or transmit defamatory material that may tarnish or damage Green Synergy reputation.

iv. make or post indecent remarks, proposals, or materials on the Internet including social networking sites that may bring Green Synergy into disrepute.

v. use the computer and/or internet to perpetrate any form of fraud, or software, film or music piracy.

vi. make contact with young people you work with at Green Synergy through personal email, personal messaging or personal social networking media profiles.

vii. to download any software – unless agreed in advance with Green Synergy's IT support service.
viii. to send or receive emails from personal email facilities offered on third party servers (e.g. such as those provided by Hotmail)

b. Files should not be downloaded from the internet unless there is a valid business reason to do so.
c. Limited personal use of the internet is permissible. However, such usage should be kept to a minimum and should not interfere with an individual's work. Users are forbidden from using the system for personal business activities.
d. Never use your own personal online profiles to contact young people. Create a separate 'work' profile with your Green Synergy email account for use when contacting young people on social networking, messaging and blogging sites.
e. As you would in a work setting, show good judgement when 'friending' someone, especially a young person online. Please refer to our GS49 Green Synergy Social Media Policy for more detailed information.
f. When using your online 'work' profile, bear in mind that you are still representing Green Synergy.
g. Use the same judgement in writing posts as you would in writing any formal letter. Post only content that you would be comfortable having the organisation, young people, your colleagues, Green Synergy's audiences and the public read, hear or see.
h. Take a shared responsibility to monitor Green Synergy websites and social networking pages. Flag up any inappropriate content and having it removed as appropriate.

12. Software Programmes

a. Participants of staff have a duty to familiarise themselves with the efficient use of the standard Microsoft Office 365 suite of programmes currently used within the Group, namely Word for Windows, Excel, PowerPoint and Outlook and Teams, making full use of the "help" elements incorporated within these programmes. Microsoft Outlook is Green Synergy standard email, diary and contacts database platform and participants of staff are expected to make themselves fully conversant with its efficient use.

13. Server Management

a. All participants of staff have a log in access that grants them direct access to the cloud hosted Team shared drive which acts as our central server. The Teams Shared

drive is for the most up to date versions of central and organisational files. SMT also have access to the Green Synergy Operational shared drive.

b. Staff SHOULD NOT duplicate central files to local folders or to their personal document files. Doing so not only uses additional and unnecessary server space but means that you may not be working from the most recent copy of a given document.

c. Staff will only have access to the files that are necessary for them to do their day-to-day work. If a permission is insufficient, contact our Chief Executive.

14. Data Protection Policy

a. Green Synergy has a legal duty under the Data Protection Act 1998 (the 1998 Act), and 2018 Act, any subsequent amendments and the General Data Protection Regulation (GDPR) to ensure we keep high standards in the handling of personal information and protect an individual's right to privacy – especially as we work with children and young people which is considered to be especially sensitive information. The Data Protection Act 1998 and the General Data Protection Regulations 2018 applies information about living individuals in electronic format and on paper. For example, this may include information such as name, address, date of birth and opinions about the individual or any other information from which the individual can be identified. This means that we should:

   i. Only hold information on young people that has a specific purpose such as because they are a member, a volunteer, a graduate or because they have agreed to be on our interviewee list.
   ii. Only hold information for as long as necessary. How long is necessary will depend on the type of funding that has supported that young person's participation.
   iii. We should have consent for any information we hold and the young people/ parent guardian should be aware of why and how we hold it.
   iv. All information should be held securely which means if we hold paper files, they need to be kept at your office in a secure lockable cabinet. Young people's information should not be left lying around or stored at home. If you make copies of a member's information – for example when going on a trip, this information should then be destroyed again at the end of the trip.
   v. If your participants information is kept electronically the spreadsheet or database should be pass worded. The password should be given out only

on a need-to-know basis and a central copy of the password held by one of the designated people.

vi. If information about young people is stored on your desktop computer make sure that you lock your computer when you leave your desk by pressing the windows key and the letter 'L'. You will need your password to get back in.

vii. If information about young people is stored on your laptop, make sure that your laptop has a start-up/ login password and that your spreadsheet/ database is passworded.

viii. Green Synergy never gives out information about the children and young people we work with except in certain safeguarding situations. If you are in a situation where you feel it would be appropriate to share information about a young person with a partner organisation, please go to the designated person for guidance first.

ix. If you are referring to a child or young person and using sensitive information in email etc please use initials.

x. Access to young people's information will be given on a need-to-know basis.

xi. NEVER share your password to a database or to your settings with another person – regardless of whether they are a colleague or not.

15. Sanctions

a. Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal. For further reference the disciplinary procedure is set out in the staff handbook. Additional action may be taken by Green Synergy and where appropriate, police may be involved, or other legal action taken.

16. Leavers Policy

a. When a member of staff leaves Green Synergy they must hand in all equipment, mobile devices and computing equipment. Green Synergy will notify JSM Computers of leavers so that their access to email, the cloud and any other systems is revoked.

17. Change to the Policy

a. Green Synergy may revise this and associated policies at any time as we make upgrades to our IT and IT security systems, in the event of legislation changes and /

or a major incident. We will notify staff of changes however you are expected to stay abreast of changes that are made, as they are legally binding.

b. This policy will be reviewed in line with an ongoing upgrade to our security procedures, in line with our Security Management Plan.

18. Agreement

a. All charity employees, contractors or temporary staff and volunteers who have been granted the right to use Green Synergy internet access and I.T. equipment are required to sign the attached agreement confirming their understanding and acceptance of this policy.

IT AGREEMENT

(Please print a copy, sign and hand it to your line manager)

All company employees, contractors or temporary staff and volunteers who have been granted the right to use Green Synergy internet access and I.T. equipment are required to sign the attached agreement confirming their understanding and acceptance of this policy.

I have read and understand the above and agree to use Green Synergy computer facilities and the internet within these guidelines.

Name:_____ Date:__/__/____

Review date: 12/09/2026

Related Documents:

- GS4 Green Synergy Children and Young People Safeguarding Policy
- GS5 Green Synergy Adults Safeguarding Policy
- GS7 Green Synergy Data Protection Policy
- GS7a Green Synergy Privacy Statement

Document Control:

Policy Details	
Policy	GS10 Green Synergy IT Management and Security Policy 2022

Version	Date of Review	Reviewed by	Approval
V1	07.10.2022	CEO	Trustee Basecamp review
V2	04.01.2023	Treasurer / CEO	Trustee Basecamp approval
V3	05.10.2023	CEO	Trustee Basecamp approval process
V4	17.09.2024	CEO	Trustee Google Drive Governance Portal
V5	12.09.2025	CEO	Trustee Google Drive Governance Portal