

Communications, Email, Internet and Social Media Policy

1. Introduction

- 1.1 This Communications, Email, Internet, and Social Media Policy applies to all employees, volunteers, trustees and contractors of Sacriston Youth Project, (“the Charity”) who use the communications equipment, computers, devices, and systems provided by the Charity (“Users”).
- 1.2 Users are encouraged to use email and the internet at work as a fast and reliable method of communication with significant advantages for business.
- 1.3 In light of the fact that communications made by Users and their other activities online reflect upon the Charity and are capable of creating a number of commercial, professional, and legal problems, this Policy is intended to clarify what the Charity expects from Users and their responsibilities when using the Charity’s communications, email, and internet facilities (collectively, “the Charity’s Internet and Communication Facilities”).
- 1.4 The Charity’s Internet and Communication Facilities include:
 - 1.4.1 Telephone / Mobile Phone;
 - 1.4.2 Email;
 - 1.4.3 Internet;
 - 1.4.4 Internal systems, such as Breathe HR etc.
 - 1.4.5 Computers; and
 - 1.4.6 Portable devices.This list is not exhaustive.
- 1.5 In addition to this Policy, when using the Charity’s Internet and Communications Facilities, Users must also comply with other Charity Policies including the Charity’s Data Protection Policy, Dignity at Work and Equality and Diversity Policy.

2. General Principles

- 2.1 There are certain general principles that should be considered when using any type of communication, be it external or internal, including hard copy letters, memos, and notices. The Charity expects all Users to:

- 2.1.1 Use the Charity's Internet and Communication Facilities, and non-electronic facilities including but not limited to Charity letterheads and stationery, responsibly and professionally and at all times in accordance with their duties;
 - 2.1.2 Be mindful of what constitutes confidential or restricted information and ensure that such information is never disseminated in the course of communications without express authority;
 - 2.1.3 Be mindful of what constitutes personal data and ensure that personal data relating to employees, clients, partners, contractors, and students is never disseminated in the course of communications unless it is used in accordance with the Charity's Data Protection Policy and with express authority;
 - 2.1.4 Ensure that they do not breach any copyright or other intellectual property right when making communications;
 - 2.1.5 Ensure that they do not bind themselves or the Charity to any agreement without express authority to do so; and
 - 2.1.6 Be mindful of the fact that any communication may be required to be relied upon in court, to the advantage or the detriment of the individual or the Charity, and to conduct their use of communication systems and equipment accordingly.
- 2.2 The viewing, transmission, downloading, uploading, or accessing in any way of any of the following material using the Charity's Internet and Communications Facilities will amount to gross misconduct with the possibility of summary dismissal:
- 2.2.1 Material, which is pornographic, sexist, racist, homophobic, or any other discriminatory or otherwise offensive material;
 - 2.2.2 Illegal or criminal material, including material which breaches copyright or any other intellectual property right;
 - 2.2.3 Any material which has the object or effect of causing harassment to the recipient;
 - 2.2.4 Material which the User knows, or reasonably ought to know, is confidential or restricted information and which they are not authorised to deal with;
 - 2.2.5 Any website or online service which the Charity has blocked access to.

3. Internet Use

- 3.1. The Charity provides access to the internet for the sole purpose of business and to assist Users in the performance of their duties. However, the Charity recognises that Users may need to use the internet for personal purposes and such use is permitted provided it is reasonable and does not interfere with the User's performance of their duties and is outside of normal working hours or during a break. Users may be asked to justify the amount of time they have spent on the internet or the sites they have visited.
- 3.2 Users must not use the internet to gain or attempt to gain unauthorised access to computer material or private databases, including restricted areas of the Charity's network. Nor must they intentionally or recklessly introduce any form of malware, spyware, virus, or other malicious

software or code to the communications equipment or systems of the Charity.

- 3.3 Users must not access or attempt to access any information which they know or reasonably ought to know is confidential or restricted.
- 3.4 Users must not access or use personal data online in any manner that is inconsistent with the Charity's Data Protection Policy.
- 3.5 Users must not download or install any software without the express permission of their Line Manager.
- 3.6 Users must not attempt to download, view, or otherwise retrieve illegal, pornographic, sexist, racist, offensive, or any other material which is in any way in bad taste or immoral. Users should note that even material that is legal under UK law may nonetheless be in sufficiently bad taste to fall within this definition. As a general rule, if any person might be offended by any content, or if that material may be a source of embarrassment to the Charity or otherwise tarnish the Charity's image, viewing that material will constitute a breach of this Policy. Any such attempt will constitute a disciplinary offence and in addition to internet access being reviewed, reduced, or withdrawn, may be subject to disciplinary action or summary dismissal.
- 3.7 Certain websites are blocked and cannot be accessed using the Charity's Internet and Communication Facilities. If a User has a genuine and specific business need to access a blocked site, they must contact their Line Manager.

4. Social Media Use - General Principles

- 4.1 This section of this Policy addresses the use by Users of all types of social network and social media platforms including, but not limited to, Facebook, Twitter, LinkedIn, Instagram, Pinterest, Tumblr, Instagram, YouTube or any other social media platform, not listed but commonly accepted as a social media platform (collectively, "Social Media").
- 4.2 The purpose of this part of Policy is to minimise the various risks to the Charity presented by Social Media usage.
- 4.3 There are certain general principles that all Users should keep in mind when using Social Media, whether for personal use or for authorised work-related purposes. All Users must:
 - a) Use Social Media responsibly and professionally, and at all times in accordance with their duties;
 - b) Be mindful of what constitutes confidential, restricted, or other proprietary information and ensure that such information is never disseminated over Social Media without the express consent of the Charity.
 - c) Be mindful of what constitutes personal data and ensure that personal data relating to employees, clients, partners, contractors, and students is never disseminated over Social Media unless it is used in accordance with the Charity's Data Protection Policy and with express authority;
 - d) Ensure that their use of Social Media does not breach any other of the Charity's policies including, but not limited to, its Data Protection Policy, Dignity at Work and Equality and Diversity Policy.

- e) Ensure that their use of Social Media does not breach any other laws, regulatory requirements, or other applicable rules set out by regulatory bodies partner and other organisations.
- f) Ensure that they do not breach any copyright or other intellectual property rights when using Social Media;
- g) Be mindful of the fact that any communication may be relied upon in court, to the advantage or detriment of the individual or the Charity and conduct their use of Social Media accordingly.

4.4 If a User is unsure as to the appropriateness of a posting or other content they wish to publish, they should speak to their Line Manager at the earliest opportunity to seek clarification.

4.5 If a User sees any content on Social Media that disparages or otherwise reflects poorly on the Charity, such content should be reported to their Line Manager.

5. Personal Social Media Use

Users may use Social Media for personal purposes during work hours at break times, provided that such usage complies with the provisions of this Policy and provided that it does not interfere with their work responsibilities or productivity. Sacriston Youth Project Social Media sites must not be used for personal use, views or comment.

6. Business Social Media Use

6.1. Certain Users may from time to time be required to use Social Media on behalf of the Charity. Users should only do so with the authorisation of their Line Manager, in accordance with instructions issued by a Line Manager, and in accordance with this Policy.

6.2 Use of Social Media for business purposes must comply with the provisions of this Policy at all times.

6.3 Users using Social Media on behalf of the Charity may from time to time be required to interact with other internet users via Social Media, for example, in response to posts or enquiries regarding the Charity. Unless the instructions issued to that User (see paragraph 6.1) specifically authorise the User to respond without further approval, the User may not respond to any such communications without the prior approval of their Line Manager. In any event, no User using Social Media on behalf of the Charity should respond to such communications, with or without prior approval, without first consulting the relevant individual and/or department unless they are fully knowledgeable of the relevant topic and suitably qualified to respond.

6.4 Social Media contacts made during the course of business are to be treated as confidential information belonging to the Charity.

6.5 Before using Social Media on behalf of the Charity, Users may require training in order to do so, or may be required to demonstrate that they have already received suitable training, either from the Charity or from a previous employer or other organisation.

7. Acceptable Use of Social Media

- 7.1 If a User makes any posting, contribution, or creation or publishes any other content which identifies or could identify the User as an employee, contractor, agent, or other member or associate of the Charity, or in which the User discusses their work or experiences relating to the Charity, the User must at all times ensure that their conduct is appropriate and consistent with their contract of employment and the corporate image of the Charity, and should bear in mind that the User owes a duty of fidelity to the Charity.
- 7.2 Unless specifically instructed to do so Users should make it clear that they are posting on Social Media as themselves, not as the Charity, and that all opinions and ideas expressed on Social Media by that User are those of the User and do not necessarily reflect the views of the Charity.
- 7.3 Unless using Social Media on behalf of the Charity, Users should not use any Social Media accounts belonging to (or otherwise associated with) the Charity.
- 7.4 Charity email addresses may only be used to sign up to Social Media websites for work-related purposes.
- 7.5 Users should always be respectful to others when using Social Media and should always be mindful of the fact that their association with the Charity may be known to anyone at any time. The conduct of all Users on Social Media may reflect on the Charity, whether positive or negative. This applies whether a User is using Social Media for business purposes or for personal purposes, whether during working hours or otherwise.
- 7.6 If a User is unsure as to the appropriateness of a posting or other content they wish to publish, they should speak to their Line Manager at the earliest opportunity to seek clarification.

8. Unacceptable and Prohibited Use of Social Media

- 8.1 Users must refrain from doing anything on Social Media or any other websites that defames, disparages, or otherwise brings into disrepute, the Charity, a User's superiors, a User's colleagues, or other related third parties. This includes, but is not limited to, making false or misleading statements and impersonating colleagues or third parties.
- 8.2 Users must ensure that their use of Social Media does not damage the Charity, its interests, or its reputation, whether directly or indirectly, in any way.
- 8.3 As under paragraph 7.2, unless specifically instructed to do so, Users must not represent themselves on Social Media as the Charity or as posting on behalf of the Charity.
- 8.4 Users may not share the following on Social Media unless specifically authorised to do so by their Line Manager:
 - a) Confidential information;
 - b) Commercially sensitive or other proprietary business information belonging to or about the Charity or any of its employees, contractors, agents, or other affiliated third parties and organisations;
 - c) Personal data relating to employees, clients, partners, contractors, and students.

8.5 Users may not use any intellectual property belonging to the Charity on Social Media (including, but not limited to, trademarks and logos) unless specifically authorised to do so by their Line Manager.

8.6 Users may not add contacts made during the course of their duties to their personal Social Media accounts without the authorisation of their Line Manager and without the express consent of the individuals involved.

9. Charity Email Use

9.1 The email address with which Users are provided by the Charity (ending in the suffix @sacristonyouthproject.co.uk) is provided for business purposes in order to facilitate information sharing and timely communication with employees, trustees, volunteers, clients, partners, contractors, and service users. Any Charity business which is conducted via email must be conducted using Charity email and is under no circumstances to be conducted through any other personal email address or account.

9.2 Users should adopt the following points as part of best practice:

- a) Before communicating via email, Users should satisfy themselves that it is the most suitable mode of communication, particularly where time is of the essence;
- b) Ensure that the email contains the Charity disclaimer notice. This should be added automatically by the email client. If it is not, Users should speak to their Line Manager immediately;
- c) All emails should contain the appropriate business reference(s), either in the subject line or in the body of the text;
- d) Emails should be worded appropriately and in the same professional manner as if they were a letter;
- e) Users should be careful not to copy an email automatically to everyone copied into the original message to which they are responding as this may result in inappropriate or unlawful disclosure of confidential information and/or personal data;
- f) Users should take care with the content of emails, in particular avoiding incorrect or improper statements and the unauthorised inclusion of confidential information or personal data. Failure to follow this point may lead to claims for discrimination, harassment, defamation, breach of contract, breach of confidentiality, or personal data breaches;
- g) All emails should be proofread before transmission, which includes ensuring that any attachments referred to in the text are actually attached and are correct and the intended recipients' email addresses are correct;
- h) If an important document is transmitted via email, the sender should telephone the recipient to confirm that the document has been received in full.

9.3 Users must not email any business document to their own or a colleague's personal web-based email accounts.

- 9.4 Use of Charity email for any personal matter is prohibited.
- 9.5 Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, pornographic, or otherwise inappropriate material in emails. If any User feels that they have been or are being harassed or bullied, or if they are offended by material received in an email from another User, they should inform their Line Manager.
- 9.6 Users should at all times remember that email messages may have to be disclosed as evidence for any court proceedings or investigations by regulatory bodies and may therefore be prejudicial to both their and the Charity's interests. Users should remember that data which appears to have been deleted is often recoverable. If secure deletion is required, for example, where an email contains confidential information or personal data, Users should follow the steps set out in the Charity's Data Protection Policy.

10. Personal Email Use

- 10.1 Users are permitted to access and use their personal email accounts only to the extent that such use is reasonable and is outside of normal working hours or during a break.

11. Charity Telephone System Use

- 11.1 The Charity's telephone lines, and mobile phones issued by the Charity are for the exclusive use by Users working on the Charity's business. Essential personal telephone calls regarding Users' domestic arrangements are acceptable, but excessive use of the Charity's telephone system and/or mobile phones for personal calls is prohibited. Acceptable use may be defined as no more than 10 minutes of personal calls in a working day. Any personal telephone calls should be timed to cause minimal disruption to Users' work.
- 11.2 Users should be aware that telephone calls made and received on the Charity's telephone lines and mobile phones issued by the Charity may be routinely monitored to ensure customer satisfaction or to check the telephone system is not being abused.
 - 11.2.1 If the Charity discovers that the telephone system or a mobile phone issued by the Charity has been used excessively for personal calls, this will be treated as a disciplinary matter and will be handled in accordance with the Charity's disciplinary procedures.

12. Personal Mobile Phone Use

- 12.1. Any personal telephone calls on Users' own mobile phones should be timed to cause minimal disruption to Users' work.
- 12.2. Only in an emergency should User's take personal calls whilst delivering activities or working directly with our members.

13. Security

- 13.1. The integrity of the Charity's business relies on the security of the Charity's Internet and Communications Facilities. Users bear the responsibility of preserving the security of the Charity's Internet and Communications Facilities through careful and cautious use. In addition to the general provisions contained in this Policy, Users must also comply with the Charity's

Data Protection Policy.

- 13.2. Access to certain websites and online services via the Charity's Internet and Communications Facilities is blocked. Often the decision to block a website or service is based on potential security risks that the site or service poses. Users must not attempt to circumvent any blocks placed on any website or service by the Charity.
- 13.3. Users must not download or install any software or program without the express permission of their Line Manager and are reminded of paragraphs 3.2 and 3.5 of this Policy.
- 13.4. Users must not delete, destroy, or otherwise modify any part of the Charity's Internet and Communications Facilities (including, but not limited to, hardware and software) without the express permission of their Line Manager.
- 13.5. Users must not share any password that they use for accessing the Charity's Internet and Communications Facilities with any person, other than when it is necessary for maintenance or repairs by the Charity's technical support team. Where it has been necessary to share a password, the User should change the password immediately when it is no longer required by the technical support team. Users are reminded that it is good practice to change passwords regularly.
- 13.6. Users must ensure that confidential information, personal data, and other sensitive information is kept secure. The security of personal data in particular is governed by the Charity's Data Protection Policy, which Users must comply with at all times when handling personal data. Workstations and screens should be locked when the User is away from the machine and hard copy files and documents should be secured when not in use.
- 13.7. If a User has been issued with a laptop, tablet, smartphone, or other mobile device, that device should be kept secure at all times, particularly when travelling. Mobile devices must be password-protected and, where more secure methods are available, such as fingerprint recognition, such methods must be used. Confidential information, personal data, and other sensitive information stored and/or accessed on a mobile device should be kept to the minimum necessary for the User to perform their duties. Users should also be aware that when using mobile devices outside of the workplace, information displayed on them may be read by unauthorised third parties, for example, in public places and on public transport.
- 13.8. Users using Charity-issued mobile devices (as outlined above in paragraph 13.7) must not connect such devices to public wi-fi networks, for example, in cafes, restaurants, and on public transport without the express approval of a particular network from their Line Manager.
- 13.9. When opening email from external sources Users must exercise caution in light of the risk malware, spyware, viruses, and other malicious software or code pose to system security. Users should always ensure that they know what an attachment is before opening it. If a User suspects that their computer has been affected by a virus they must contact their Line Manager immediately.

14. Monitoring

- 14.1. To the extent permitted or required by law, the Charity may monitor Users' use of the Charity's Internet and Communications Facilities for its legitimate business purposes which include (but

are not necessarily limited to) the following reasons:

- a) To ensure Charity policies and guidelines are followed, and standards of service are maintained;
- b) To comply with any legal obligation;
- c) To investigate and prevent the unauthorised use of the Charity's Internet and Communications Facilities and maintain security;
- d) If the Charity suspects that a User has been viewing or sending offensive or illegal material (or material that is otherwise in violation of this Policy);
- e) If the Charity suspects that a User has been spending an excessive amount of time using the Charity's Internet and Communications Facilities for personal purposes.
- f) If the Charity suspects an employee of activity that is illegal, will bring Sacriston Youth Project into disrepute or damage reputation.
- g) If the Charity suspects an employee of activity that brings commercial risk.

The list is not exhaustive.

14.2. Users should be aware that all internet and email traffic data sent and received using the Charity's Internet and Communications Facilities is logged, including websites visited, times of visits, and duration of visits. Any personal use of the internet will necessarily therefore be logged also. Users who wish to avoid the possibility of the Charity becoming aware of any political or religious beliefs or affiliations should avoid visiting websites at work which might reveal such affiliations. By using the Charity's Internet and Communications Facilities for personal use, Users are taken to consent to personal communications being logged and monitored by the Charity. The Charity shall ensure that any monitoring of Users' use of the Charity's Internet and Communications Facilities complies with all relevant legislation including, but not limited to, the GDPR (EU Regulation 2016/679 General Data Protection Regulation) and the Human Rights Act 1998.

14.3. When monitoring emails, the Charity will normally restrict itself to looking at the address and heading of the emails. However, if it is considered necessary, the Charity may open and read emails. Users should be aware that sensitive and confidential communications should not be sent by email because it cannot be guaranteed to be private.

15. Recruitment

The Charity may use internet searches to carry out due diligence as part of its recruitment process. In these circumstances, the Charity will act in accordance with its equal opportunities and data protection obligations.

16. Misuse and Compliance

16.1. Any User found to be misusing the Charity's Internet and Communications Facilities will be treated in line with the Charity's Disciplinary Policy and Procedure which in some cases can constitute gross misconduct. Misuse of the internet can, in some cases, amount to a criminal

offence.

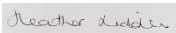
16.2. Where any evidence of misuse of the Charity's Internet and Communications Facilities is found, the Charity may undertake an investigation into the misuse in accordance with the Charity's Disciplinary Policy and Procedure. If criminal activity is suspected or found, the Charity may hand over relevant information to the police in connection with a criminal investigation.

17. Review and Training

17.1 The Charity will provide data protection training to all employees on a regular basis.

17.2 This policy will be reviewed on an annual basis.

This policy has been approved & authorised by:

Name: Heather Liddle
Position: Trustee – Sacriston Youth Project
Date: April 2021
Signature: 

Date of Review	Reviewed By	Changes Made	Date of Next Review
April 2021	Jo Cameron - Trustee		April 2022