Acceptable Use Policy (AUP)

Record of updates

Acceptable Use policy	
Date Created	**1 May 2020**
Revision Due	**July 2022**
Revision Due	**May 2023**
Revision Due	**November 2024**
Revision Due	**January 2026**

DOCUMENT VERSION CONTROL		
Issue No.	**Issue Date**	**Summary of Changes**
1	May 2020	Merged One West policy with RISE Social networking policy
2	May 2022	DPO agreed. Added 2 factor authentication
3	November 2023	No updated policy sent by DPO – no amendments required
4	January 2025	Updated according to OneWest master policy

THE RISE TRUST

1. Introduction

Information is a vital asset to The RISE Trust, without which it would be unable to provide effective and efficient services to children, young people and families. This policy is designed to provide users with a full understanding of the appropriate use of trust systems safely, securely, and efficiently.

2. Scope

Users are defined as all Employees, Bank Staff, Trustees, Consultants, Contractors and any other person or organisation acting for or on behalf of the trust who have been granted access to trust Systems and the data used in performance of any purpose for which access was granted.

a) Systems include but are not limited to all of the trust physical assets, e-mail accounts, Instant Messaging, any Internet or Intranet sites, facsimile, voice mail and telephone (fixed or mobile) equipment.

b) All Users must make themselves familiar with the appendices which give more detailed guidance over use of the trust electronic communications systems.

3. Key Principles

a) All 'Users' must make themselves aware of the guidelines attached to this policy, which provide more detailed explanations.

b) All 'Users' are encouraged to use the most efficient and effective communication tools to fulfil their duties which includes e-mail, use of the Internet, Instant Messaging, and phone systems.

c) All systems, as identified in paragraph 2(a) above, are wholly owned by the trust, and as such are primarily for business use.

d) All 'Users' should only use these systems for business use, however minimal personal use of these systems is permitted as outlined in Appendix One. Only in the most exceptional circumstances - i.e. an urgent health matter - should bank staff, consultants, contractors and any other persons or organisations acting on behalf of the trust be allowed to use these systems for personal use.

e) Whilst minimal personal use is permitted it must not be excessive, inappropriate or interfere with carrying out contractual responsibilities and not adversely affect either the trust business or reputation or place the trust at unnecessary risk.

f) The trust maintains the right and ability to monitor and scrutinise any data within its systems (as detailed in paragraph 2(a) above) and 'Users' can have no expectation of privacy for anything that is created, stored, sent or received via the trust systems.

g) E-Mails should not be retained for longer than 12 months, unless it either constitutes a trust Record, in which case it must comply with the Retention of Records Policy, or there is a clear business need for retention.

h) Users must make themselves aware that use of the trust Systems is subject to a number of key statutory responsibilities, i.e. Freedom of Information Act and this requires appropriate standards to be applied by Users as detailed in the attached guidelines.

i) 'Users' are reminded that specific care must be taken when issuing and receiving information and attachments from external sources and the guidelines must be followed.

j) Failure to adhere to this policy and attached guidelines may result in withdrawal of these systems from a 'User' and/or action under the trust Disciplinary procedure

4. Monitoring & Review

a) Should it be discovered that this Policy has not been complied with, or if an intentional breach of this Policy has taken place, senior management shall have authority to take immediate steps as considered necessary, including disciplinary action.

b) The policy will be subject to ongoing review in light of any changes in legislation or good practice, and will be formally reviewed on a periodic basis, and at least annually.

c) The trust, through Oakford IT Support, will employ monitoring software to inspect and review information within its systems.

APPENDIX ONE - ACCEPTABLE USE GUIDELINES

Table of Contents

Introduction

1. These guidelines define acceptable use of the RISE Trust's email, intranet/internet access points, use of devices (personal, as well as those that belong to the trust) and the use of social media. They describe broad trust principles regarding acceptable use and may be supported by further documentation covering aspects of the trust's information systems and services.

2. Any communications using these systems represent the trust. Therefore, you should ensure that all messages, communications and information created by you are professional in tone and content. The style and language of any messages,

communications or information that you create should be in accordance with the Trust's staff behaviour policy.

3. Subject to the provisions set out in the section covering personal of the Trust's Devices and Communications methods, you are not allowed to use the systems for any reason other than for genuine trust purposes. The systems are provided as business tools and any complaints or allegations of misuse and misconduct will be dealt with in accordance with the trust's Disciplinary Procedure. The trust retains the right to remove access to these facilities if they are either misused or form the basis of misconduct.

Email

4. Care must be applied prior to the release of any e-mail, or attachment, however inconsequential the contents might appear to be, to ensure that the legislative requirements and these policy standards are complied with. Users should only direct e-mails to persons who need to know the information that they contain and should only send general messages to a group of persons where it is strictly necessary to do so.

5. The copying of e-mails where not required is discouraged, and confirmation of receipt is to be obtained for important e-mails sent. The unnecessary inclusion of attachments, particularly ones that are sent internally, is also discouraged.

Retention of Relevant Data

6. E-mails and other electronic communications have the same status as any other trust record and are to be treated in accordance with all associated RISE policies relating to topics, such as data protection and safeguarding etc. Such communications, where they are kept as a trust record, are liable for disclosure in response to information access requests under current legislation, for example the Data Protection Act 2018 and Freedom of Information Act 2000.

7. No e-mail or other electronic transmission should be retained for longer than 3 months unless:

   a. It either constitutes a RISE trust Record, in which case it must comply with the Retention of Records Policy; or,
   b. There is a clear business need for retention.

8. All users must therefore be familiar with the trust Records Management and Retention of Records Policies and act in accordance with the standards outlined in these documents.

Email Etiquette

9. To promote good practice the trust recommends the adoption of the following etiquette rules for three main reasons:

   a. **Professionalism**: Using proper e-mail language will help put across a professional business image.
   b. **Efficiency**: E-mails that get to the point are much more effective than poorly worded e-mails.
   c. **Protection from liability**: Employee awareness of e-mail risks will help protect the trust and mitigate risks.

10. There are many email etiquette rules. These are the ones that the RISE Trust recommends.

a. System Use

It is The RISE Trust policy that e-mail should be read on a regular basis and all correspondence is to be dealt with at least to the standards outlined in trust Communications Policy or best practice for postal communications.

- i During any absence arrangements are to be made that ensure messages can be diverted to a suitably authorised manager.
- ii Use Outlook Out of Office where appropriate.
- iii Before sending an email consider whether e-mail is the most appropriate method for communicating.
- iv Do not impersonate any other person when using e-mail.
- v Do not access a web site direct from an e-mail link.
- vi Do not create-mail congestion by sending trivial messages to users.
- vii Users are to be cautious when accepting e-mails – it is not difficult to fake both content and sender.
- viii Users should check that the content provides reasonable assurance of its authenticity and should consider checking by alternate means that it has come from its purported sender.

b. Content

- i Be concise .and to the point.
- ii Answer all questions and try to pre-empt further questions.
- iii Make it personal.
- iv Use templates for frequently used replies.
- v Keep to the message thread.
- vi Use a meaningful subject.

c. Style, Tone and Format

- i [Font should be Arial, style Regular, size 12 and black in colour except where otherwise required by the recipient].
- ii [Background should be white rather than any other colour or personalisation of the page].
- iii Use proper spelling, grammar and punctuation.
- iv Use a proper structure and layout.
- v Do not write in CAPITALS – it could be construed as shouting.
- vi Consider the appropriateness of the use of acronyms, abbreviations and emoticons.
- vii Use active rather than passive language.
- viii Avoid long sentences and consider the length of the e-mail.
- ix Do not send or forward e-mails or attachments with prohibited material.
- x Keep your language gender neutral.
- xi Consider the wording used upon starting and ending the e-mail.
- xii Use email signatures that include The RISE Trust name, job function, telephone, mobile, working hours and address.
- xiii Avoid sending confidential, sensitive or personal information by e-mail.
- xiv Never send confidential messages by e-mail without getting the recipients agreement.

d. Options

- i Do not overuse the high priority option.
- ii Use blind carbon copy (BCC) when emailing multiple external recipients (for example parents) – this will ensure they cannot see each other's email addresses.
- iii Ensure that the e-mail has an appropriate disclaimer.
- iv Do not overuse the Reply to All.
- v Do not overuse Group or All Mail User options.
- vi Use the cc field sparingly, carefully considering the need for others to receive it.
- vii Do not print out e-mails without considering the need for a hard copy.

e. Replies

- i Answer swiftly and in accordance with trust standards.
- ii Do not forward chain, pyramid or similar schemed e-mails.
- iii Do not copy an e-mail or attachment without careful consideration of need.
- iv Do not forward virus hoaxes. Instead inform the Information Security Office or IT provider of receipt.
- v Do not reply to unsolicited bulk e-mail, known as spam.
- vi Do not abuse others, even in response to abusive e-mails received.
- vii In a reply state clearly, what is required of the recipient.
- viii If a recipient asks you to stop sending them personal messages, then always stop immediately.

f. Attachments

- i Do not attach unnecessary files.
- ii Check any attachments to ensure they do not contain information which should not be disclosed (e.g. in other worksheets, overwritten templates).
- iii Make use of trust bulletin boards and/or the intranet where there is a need to copy e-mails and documents to a wider audience.
- iv [Wherever possible send links to documents held in a 'shared' area rather than send an attachment].
- v Never open an e-mail attachment from an unexpected or untrustworthy source.

g. Before Sending

- i Read your e-mail carefully and consider the content before sending.
- ii Consider how the recipient will interpret the message and ensure your intention is clear.
- iii Imagine that you are talking to them face to face.
- iv Retain copies of important e-mails, bearing in mind trust policy on records retention.
- v Ensure that the address is correct, particularly when using auto-fill, if using bcc ensure that it correctly completed. This is the largest cause of data breaches in the trust. Hence pay very close attention to this point.

h. Deleting e-mails

i When deleting e-mails users must ensure they ‘double delete’ as a minimum. This means that after deleting you must access the deleted items folder and delete them again.

ii To be completely sure an e-mail is deleted you must then use the toolbar to access the option ‘Recover deleted items’

iii This will highlight all those e-mails you have double deleted and then you can purge these double deleted e-mails from the system so that they can no longer be recovered.

Internet Use

11. Users are to ensure that their use of the Internet does not affect the trust in any adverse manner. If users are in any doubt as to the appropriateness of their use of the Internet, further support and advice is to be sought from senior management.

12. It is acknowledged that the Internet is totally unregulated and uncensored, but the trust expects all Internet access to be conducted in compliance with the Acceptable Use Policy. Failure to comply with the rules set out in the Policy may result in legal claims against the user and the trust and may lead to disciplinary action being taken against the user.

13. The costs and consequences of inappropriate use of the Internet can take many forms, but most commonly they affect the trust in terms of:

a. loss of productivity.
b. impact on network resources.
c. security issues.
d. legal liability.
e. adverse publicity.

14. For acceptable personal use see paragraphs 51-57.

Device Use

Mobile Phone

15. Again, personnel communicating with parents/carers, third-party suppliers and external organisation/s with trust devices represent the trust. Hence, users should ensure that all messages and communications created are professional in tone and content. The style and language of any messages and communications that are created should be in accordance with standard business communications, see e-mail etiquette above for hints and tips.

16. Care must be applied prior to the use of mobile phones, however inconsequential the subject of the communication might appear to be, to ensure that legislative requirements and these standards are complied with.

17. Users should only direct communications to person who need to know the information that they contain and should only send text messages to a group of persons where it is strictly necessary to do so.

18. Staff must not use mobile phones in any manner that may put them, other staff or members of the public at risk.

19. Users must be aware of their surroundings when using the device, especially when the device is displaying information that may be considered person-identifiable, sensitive and/or confidential information.

20. Always check that the person you are calling is able to talk safely, i.e. they may be on site or driving. Staff must not use a mobile phone whilst driving. It is an offence to do so, and they may be personally prosecuted and/or fined for doing so.

21. Whilst use of Bluetooth and car kits is allowable, it is not promoted. Phones should ideally be turned off and any messages retrieved at the end of the journey, when it is safe to do so.

22. Disciplinary action may be taken if a member of staff uses their mobile phone in a manner that puts them, staff or the public at risk.

23. Users are responsible for the day-to-day security of mobile phones issued to them:

  a. Whilst in the office, store the phone and associated equipment with due care. Do not leave the phone unattended on a desk.
  b. Secure it at home as if it is a personal possession. Never leave it in an unattended vehicle.
  c. When not in use activate the keypad lock.
  d. Set a PIN code to prevent unauthorised use (this is particularly important if you maintain any sensitive records such as contact details for vulnerable clients on the phone).

24. When saving contacts onto your phone they must be saved to the sim card and not to the phone. This safeguards against phone damage as contacts are not lost with the phone, as well as allowing a smooth transfer of numbers during the upgrade process.

25. When returning a phone that is no longer required all saved data, e.g. messages and contacts must be deleted, use the factory condition function if available. The pin code must be set to 0000 when returning the phone or a sticker with the pin code attached to the phone.

Device Use Security

26. When making use of trust devices and systems users must ensure that passwords/PIN codes are safeguarded and not, accidentally, or deliberately, disclosed for use by others. When not in use, activate the keypad lock on the phone or lock the screen on the laptop. Set a PIN code to prevent unauthorised use of the phone (this is particularly important if you maintain any sensitive records such as contact details for vulnerable individuals on the phone.

27. Users are responsible for the day-to-day security of trust equipment. Where the items are portable and of higher risk of theft, i.e. mobile phones or laptops, reasonable steps to safeguard them must be taken.

28. Whilst in the office, store the phone/laptop and associated equipment with due care. Do not leave the phone unattended on a desk and ensure laptops are secured overnight.

29. Appropriately secure the phone and laptop at home as if is a personal possession. Do not lend the phone or laptop to anyone else.

30. Proven breaches of these security requirements, which are defined in more detail in the trust Data Breach Policy, may lead to action being taken under the trust Disciplinary Procedure.

31. Please refer to the trust Information Security Policy, or senior management for further details. Advice and support is also available from the trust DPO.

Device Use Scanning of Documents

32. The following general principles must be followed when scanning original documentation:

a. Scans done via Multi- Function Devices (MFD) must be scanned as a PDF, must be scanned to email and saved to a managed system. The email must be deleted once the scan is saved. The use of Scanned Files folders is not recommended due to the lack of access controls (see paragraph 38).

b. Scans done via a stand-alone machine must be scanned as PDF and saved to a managed system.

c. The scanned document must be checked against the original to ensure an accurate and complete copy.

d. The scanned document must be managed in accordance with Records Retention Schedules.

Multi Functioning Devices (MFD)

33. Any documents scanned via a MFD must be scanned as a PDF and where possible the MFD will be set to scan as a PDF as default, with no option to change.

34. Any documents scanned via a MFD must be scanned to email. Any new MFD's within the trust will be set to scan to only the user's work email address as default without the option to change. Once the document is scanned to the user's work email address, users must save the document to a managed system. The scanned document should be saved with the relevant Metadata (date & description in the title) and wherever possible a unique identifier. No personal identifiable data should be used in the document title.

35. Once the scanned document has been saved to a managed system the email containing the scanned document must be deleted.

Networked Devices

36. Any correspondence or photographs scanned via a network scanner must be scanned as a PDF. Drawings and plans may be scanned as a .tif file but must be converted to a PDF file before making them public.

37. The scanned document must be indexed with the date & description in the title (aka metadata) and wherever possible, a unique identifier that does not contain personal identifiable information.

38. To ensure the confidentiality of scanned documents uploaded to a shared repository or application it is essential that the documents are only visible to those with proper authorisation. Due consideration should therefore be given to reviewing the security of the scanner functionality and application to protect the information.

Stand-Alone devices

39. Any documents scanned via a stand-alone device must be scanned as a PDF.

40. The scanned document must be saved to a managed system and must not be saved to a generic folder. The scanned document should be saved with the date & description in the title (aka Meta Data) and wherever possible a unique identifier. No personal identifiable data should be used in the document title.

Original Documents

41. The original source document should generally be destroyed after it has been scanned, to avoid duplication and minimise administration. However, in exceptional cases there may be reasons why the document should be retained. If in doubt as to whether an original document should be retained, users should consult the Records Retention Policy, the CEO or the DPO.

42. The original document must be managed in accordance with Records Retention Schedules.

43. All scanned documents must be checked to ensure the scanned image is an accurate and complete copy of the original source document.

44. Whether a document is scanned via the methods detailed above, any further transfer of the document must be done with due consideration and care as to the sensitive and confidential nature of the contents of the document.

Scanned Documents and Legal Compliance

45. Scanned documentation may be used in legal cases and the following information clarifies the viability for the use of scanned documentation

a. Civil cases - Section 8 of the Civil Evidence Act 1995 states:
Proof of statements contained in documents
i. Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved.
(1) By the production of that document, or
(2) Whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such a manner as the court may approve.

46. Therefore, documentary evidence in the form of electronic documents, including scanned documents, will almost always be held as legally admissible.

47. Criminal cases - Section 71 of the Police and Criminal Evidence Act 1984 states:

> *In any proceedings the contents of a document may (whether or not the document is still in existence) be proved by the production of a microfilm copy of that document or of the material part of it, authenticated in such a manner as the court may approve.*

48. Ultimately an original document will always hold more weight than a copy. In fact, copies are referred to as ‘secondary evidence’. However, if it can be demonstrated through robust processes and audit that a document is an authentic and true copy of the original, it will have almost the same weight as the original and it is unlikely it will be challenged.

49. The Current British Standard is BSI 10008:2014 – Legal Admissibility and Evidential Weight of Information Stored Electronically. This sets the benchmark for procedures that should be followed to achieve best practice, and therefore the legal admissibility of electronic documents.

50. The scanning of any document for which a third party holds the copyright must comply with the Copyright, Designs & Patents Act 1988. Copyright applies equally to paper documents, electronic information, CD-ROMs, websites, images, computer programs etc.

Personal Use of trust Devices and Communication Methods

51. The hardware, software and materials relating to electronic communications are owned wholly by the trust, which has developed these to facilitate effective business communication within the workplace and as such are primarily for business use.

52. Personal use of the trust mobile phones or systems to send e-mails or to browse the Internet is permitted, but should be on a minimal basis only, and is defined below. Inappropriate or excessive use of such systems for personal use will be dealt with as a disciplinary issue.

53. When using electronic communication systems (e-mail, internet and mobile phone) for personal use, users are to ensure that:

a. The usage is minimal and takes place substantially out of normal working hours and not at other times when the employee is purporting to fulfil his/her contractual responsibility to work;

b. Whenever it takes place, it does not interfere with trust business commitments, adversely affect trust systems or harm the trust reputation.

c. It does not incur any additional expense to the trust; where it does, i.e. where the trust is liable for calls and text charges which relate to personal use then these costs must be reimbursed to the trust;

d. The usage is appropriate. Personal use of mobile phones is permitted where there is an urgent matter, such as the health of themselves or immediate family or a change in working circumstances, i.e. need to unexpectedly work late. There is no expectation that such calls should be paid for by the individual;

e. Use at all times complies with section 'Prohibited Use';

f. Use is at your own risk and the trust accepts no responsibility for any loss or disclosure of personal e-mail or attachments;

g. E-mails make it clear that the opinions expressed are your own and not the trust. To that effect all personal e-mails must also include at the start or sign off a disclaimer to this effect;

> *Personal e-mail". The views, comments expressed and transaction details contained within this e-mail are personal and are not those of trust. This e-mail is the personal responsibility of the sender. "*

h. You do not use trust facilities for any for-profit business or commercial gain.

i. Non-commercial personal procurement, such as the purchase of tickets by e-mail and the use of Internet web sites, is on a minimal basis only. The use of a trust e-mail address for this purpose is to be accompanied by a disclaimer as outlined above.

54. Personal e-mails blocked by the trust content filtering routines will not be released to the recipient. The trust has implemented measures to protect the systems in accordance with this Policy and will not employ resources to the release of such e-mails. Business e-mails will continue to be released upon request, once proof of business content and need has been established.
55. If in doubt as to whether the intended use is permissible, advice should be sought from the IT provider, senior management or DPO before proceeding.
56. In respect of the Data Protection Act 2018, employees using the Internet for personal purposes are Data Controllers in respect to the processing of personal information. As Data Controllers in these circumstances, employees are responsible for ensuring that personal data is processed in line with the principles of the Act.
57. Any complaints or allegations of misuse and misconduct may be dealt with in accordance with the trust Disciplinary Procedure.

Prohibited Use

58. Every user must ensure that all electronic communications activities are not illegal, inappropriate nor contrary to the good conduct of trust business. To ensure compliance, it is trust policy to prohibit certain activities. Users must not use the trust Systems to:

a. Create, review or transmit material that is inappropriate, offensive, untrue, defamatory, malicious, racist or disruptive in nature. In particular, you are not permitted to create, review or transmit material containing discriminatory, harassing or threatening comments, or any other form of communication that is contrary to trust Policies. These include, but are not limited to, the trust Equality, Diversity and Inclusion, Harassment & Bullying, Data Protection and Freedom of Information Policies;

b. Spread gossip, send chain mail letters, or copy or send material in breach of copyright.

c. Download programs or any other software from the Internet.

d. Create, review or transmit jokes, stories or cartoons.

e. Open any e-mails which do not appear to be related to trust business and seem to contain jokes, graphics, or images as such e-mails regularly contain viruses, or

f. Play computer games.

59. Any complaints or allegations of misuse and misconduct may be dealt with in accordance with the trust Disciplinary Procedure.
60. The following section provides more detailed guidance on what the trust deems to be unacceptable in terms of electronic communications and defines the wording of many of the terms used above:

a. **Defamation.** Defamation is the documenting of an untrue (libellous) accusation which adversely effects the professional and/or personal reputation of an individual(s) and is an offence under U.K. legislation. It is there prohibited to send, access or transfer information or messages whose content or intent would reasonably be considered to be abusive, disrespectful, hurtful or undermining in nature. The communication of information regarding alleged professional and/or personal misconduct is also to be avoided.

b. **Discrimination and Harassment.** Treating a person or group less favourably than another person or group is treated, based on their age, disability, gender, race, religion/belief or sexual orientation and it cannot be shown that the treatment in question was justified.
c. **Harassment.** Conduct by one person to another, which is unwanted, unreasonable and offensive to the recipient. The trust is committed to the creation of a working environment free from discrimination and harassment, and this is supported by the Equality Commitment, Equal Opportunities and Harassment & Bullying Policies.

Inappropriate Material

61. The use of trust facilities to knowingly create, view, read, download, upload, distribute, circulate or sell material which is pornographic, sexually explicit, obscene, racist, sexist, violent in nature or which is criminal in nature/content is prohibited. This definition is intended to be interpreted very widely: content may be perfectly legal in the UK yet in sufficient bad taste to fall within this prohibition. Sometimes the content may be against the law. In general, if any user (intended to view the web page or not) might be offended by the contents of a web page, or the fact that the trust software has accessed the web page might embarrass the trust if made public, then it may not be viewed.

62. Inappropriate material also includes disclosure of private and personal information without consent.

63. The trust will not enter into discussions regarding the point at which sexually explicit material may be classified as pornography. There is no personal or business justification for access to websites providing such material or for those users effecting the, inward or outward, transmission of sexually explicit e-mails and/or attachments.

Copyright

64. Copyright confers upon its owner exclusive rights with regard to the publication of written material and the use of computer software. These rights are enforceable in law under the Copyrights, Designs and Patents Act 1988. It is easy to attach copyright material to e-mails and to employ cut and paste techniques and care should be taken when employing such procedures. Individuals should be aware that non-compliance with the Act may result in prosecution through the courts.

65. It is also to be noted that staff, neither own the documents they create using trust equipment, or do they have intellectual property rights therein.

Computer Misuse

66. It is forbidden to use trust facilities to undertake any action that is contrary to the Computer Misuse Act 1990. This Act specifies offences for attacks on computer systems and/or information. It provides protection for systems and data, attempting to maintain confidentiality, integrity and availability, and provides for three distinct offences:

a. Unauthorised access to computer material.

b. Unauthorised access with intent to commit or facilitate the commission of further offences.
c. Unauthorised modification of computer material.

67. Protective measures against computer malicious programs (malware) have been taken by the trust and users are reminded that it is prohibited to design, write, release, download, or attempt to download, any category of malware, including viruses, Trojans, worms and spyware.

Software and Document Downloads

68. The trust has adopted a corporate standard desktop so that all software is correctly installed and properly licensed. It is prohibited to download programs or any other software.

69. If you consider that there is a business need for non-standard software please contact the relevant member of management or the IT HelpDesk for advice.

70. Document downloads are permissible, but as such must comply with legislative requirements and are subject to the trust filtering routines.

Impersonation

71. It is prohibited to add, remove or modify identifying e-mail header information in an effort to deceive, mislead or fail to accurately identify the sender. Although the trust acknowledges that users are often unable to control the flow of e-mails and Internet transmissions into the network, users have a responsibility to ensure that inappropriate or offensive communications are deleted from PCs. PCs can be used, and screens viewed by any individual so it is essential that users are aware of their roles and responsibilities and comply with trust policy.

72. If users are in any doubt as to the appropriateness of material, they are accessing or if they are receiving inappropriate or offensive communications and material they are to inform the CEO as soon as possible.

73. Any complaints or allegations of misuse and misconduct may be dealt with in accordance with the Trust Disciplinary Procedure.

Contracts

74. The trust has detailed procedures to be followed when procuring goods and services. Where any goods/services are purchased over the Internet consideration should be given to only using a trust [Purchasing Card].

Social Media

75. Social media is the term commonly given to websites, online tools and other interactive digital tools that allows users to interact with each other, by sharing information, opinions knowledge and interests. These include:

a. Social networking utilities, such as Facebook, Instagram, X (Twitter)
b. Online discussion forums.
c. Collaborative spaces
d. Media sharing services, such as Flickr and YouTube
e. Blogs, (personal Web Logs), such as Blogger
f. Microblogging applications, such Twitter.

76. It is important that everyone uses the technologies and services effectively, flexibly and in an appropriate manner. However, with these new technologies comes added responsibilities for users of social media, both while they are at work and at home to act in a way that does not compromise the trust reputation.

77. All users should bear in mind that information they share through social media applications, even if they are on private spaces, is still subject to:

a. Copyright, Designs & Patents Act 1998
b. Data Protection Act 1998
c. Freedom of Information Act 2000
d. Safeguarding Vulnerable Groups Act 2006
e. The trust Equality, Diversity and Inclusion Policy.

Authorised Users of Social Media

78. Use of social media, on behalf of the trust, is to be used only by:

a. Those people who have been identified as media spokespeople with the agreement of the CEO and the Communications and Marketing Manager where applicable.

b. Other users who have a specifically defined role, have had a business case approved and have been appropriately trained. These business cases must have the support of the appropriate Senior Manager.

c. Users who have been given responsibility as part of managing an emergency.

79. For those people authorised to respond on behalf of the trust, training will be provided. Although social media is more conversational than other forms of communication it should be treated in an equally professional way.

80. Staff authorised to speak on behalf of the trust should ensure that they comply with paragraphs 82-84 of this policy and all other legal requirements. Those people who wish to respond in their own personal and private capacity should ensure that they comply with the guidelines in the section below.

81. Social media sites are currently blocked when using trust desktops and laptops but can be made available subject to approval.

Using Social Media on Behalf of The RISE trust

82. Social media, on behalf of the trust must not be used to:

a. Publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the trust into disrepute.

b. Be used for party political purposes or specific campaigning purposes.

c. Be used for the promotion of personal financial interests, commercial ventures, or personal campaigns.

d. Be used in an abusive or hateful manner.

e. Be used for actions that would put trust users in breach of trust codes of conduct or policies.

f. Breach the trust misconduct, equal opportunities or bullying and harassment policies.

g. To release information that could be considered confidential; or
h. Damage the trust reputation.

Correct Use of Social Media for RISE Trust Business

83. Where authorised individuals from key partners and/or external organisations are acting on behalf of the trust, they will also be expected to comply with all relevant trust Policies and associated Guidelines.

84. It is also important to ensure that members of the public and other users of online services know when a social media application is being used for official trust purposes. To assist with this, all users must adhere to the following requirements:

a. All links should be to the trust website or other approved sites.
b. The Organisation domain email address should be used for official trust purposes, unless otherwise agreed by the relevant trust CEO;
c. The use of the trust logo and other branding elements should be used where appropriate to indicate the trust support or where the trust responds formally.
d. The logo should not be used on social media applications which are unrelated to or are not representative of the trust official position.
e. Staff representing the trust should identify themselves as such where appropriate –on social media applications i.e. through providing additional information in user profiles. It is not considered appropriate for trust officers acting on behalf of the trust to deceive, even inadvertently, other users of social media.
f. They should ensure that any contributions they make are professional and uphold the reputation of the trust.
g. Comply with all the relevant legislation and the trust policies on IT.
h. They must not promote or comment on political matters or issues that may be regarded as such.
i. Avoid endorsements that are not relevant to the operation the trust.
j. Be aware that all information that you post on behalf of the trust may be subject to the Freedom of Information Act.

Using Social Media in a Private and Personal Capacity

85. The trust understands that staff may use social media, on their own equipment in their own time, for their own private use. These guidelines do not mean that staff can never post comments on these websites about their work for the trust.

86. However, before posting comments, staff should always remember that information posted on these websites becomes public knowledge and may be viewed by colleagues, service users, members of the public and the press. The trust also routinely monitors comments made about it, in social media.

87. Staff must not connect with current children/ young people on social media. Staff may wish to mask or edit their username in order to hinder children/ young people from locating them on social media platforms. For more information see the trust E-Safety and Safeguarding Policies.

88. Unless staff are authorised to speak on behalf of the trust, outside of their work time they should:

a. Use a disclaimer to make it clear that their views are their own and not necessarily the trust.
b. Avoid any actions that would put trust users in breach of trust codes of conduct or policies.
c. Avoid publishing or passing on links to any defamatory and/or knowingly false material about the trust, your colleagues and/or customers, and care should be taken to avoid using language which could be deemed offensive to others.
d. Not breach the trust misconduct, equal opportunities or bullying and harassment policies.
e. Not reveal confidential information relating to his/her employment within the trust.
f. Not say anything that would damage the trust reputation.

Other Guidelines

89. When using social media in a private and personal capacity users should also follow the guidelines suggested by the social media sites for their own safety. These can normally be found on the information pages of each social media site. Staff should:
a. Take great care how they are perceived, as the boundaries between their professional life and private life can become blurred in social networks.
b. Consider whether they would be happy for their colleagues, managers or service users to read the comments, and consider what their reaction might be.
c. Show respect for others. You should be respectful of the trust and your fellow employees. Ensure that privacy and the feelings of others is respected at all times.
d. Obtain the permission of individuals before posting contact details or pictures.
e. Not use sites for accessing or sharing illegal content; and
f. Use social media in a responsible fashion and avoid giving out personal information about you or your family.

Using Social Media in Connection with Vulnerable People

90. There will be additional requirements when dealing with particularly vulnerable groups and you should also refer to any additional guidance that has produced in these instances.

91. Staff working with vulnerable people will need to be especially vigilant and undertake safe on-line behaviour. Management may issue specific guidelines or codes of conduct to meet individual concerns related to the nature of their area.

Breaches of this Policy

92. The trust takes the approach to social media very seriously and any breach of this policy could lead to disciplinary action.

93. If it is believed that the trust has been brought into disrepute this may constitute misconduct or gross misconduct and disciplinary action will be applied as appropriate.