THE RISE TRUST

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	
Revision Due	

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

Introduction

1. 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 The RISE Trust systems safely, securely, and efficiently.

Scope

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

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

4. All Users must make themselves familiar with the appendices which give more detailed guidance over use of The RISE Trust electronic communications systems.

Key Principles

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

All adults working with children and young people have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children and young people, public in general and all those with whom they work in line with the agency's code of conduct. Adults in contact with children and young people should therefore understand that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

The RISE Trust has in place clear policies relating to child protection; allegations management; use of both personal and agency equipment i.e. emails addresses; camera's etc. This will help ensure that individuals are aware of expectations regarding interaction and contact with children.

6. All 'Users' are encouraged to use the most efficient and effective communication tools to fulfil their duties including e-mail, Microsoft Teams, use of the Internet, Instant Messaging, social media and phone systems.

7. All systems, as identified in paragraph 3 above, are wholly owned by The RISE Trust, and as such are primarily for business use.

8. All 'Users' should only use these systems for business use, however minimal personal use of these systems is permitted as outlined in Appendix A, 51-57. Only in the most exceptional circumstances - i.e. an urgent health matter - should temporary staff, consultants, contractors, volunteers and any other persons or organisations acting on behalf of The RISE Trust be allowed to use these systems for personal use.

9. 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 RISE Trust business or reputation or place The RISE Trust at unnecessary risk.

10. The RISE Trust maintains the right and ability to monitor and scrutinise any data within its systems (as detailed in paragraph 3 above) and 'Users' can have no expectation of privacy for anything that is created, stored, sent or received via The RISE Trust systems.

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

12. Users must make themselves aware that use of The RISE Trust Systems is subject to a number of key statutory responsibilities, i.e. Freedom of Information Act 2000 and this requires appropriate standards to be applied by Users as detailed in the attached guidelines.

Adults should never make a 'friend' of a child or young person on their personal social media. Where the adult is working on with a young person on their professional social networking page staff should not become 'friends' with children or young persons that are no longer receiving a service. Working to the Trust's policy on this will assist in reducing the possibility that being 'friends' with a young person no longer in receipt of services will be called into question.

13. '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.

14. Failure to adhere to this policy and attached guidelines may result in withdrawal of these systems from a 'User' and/or action under The RISE Trust Disciplinary procedure

Monitoring & Review

15. 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.

16. 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.

17. The RISE Trust, through IT Services, will employ monitoring software to inspect and review information within its systems.

Review this Policy May 2022

Appendix A

ACCEPTABLE USE GUIDELINES

Contents

1. The following areas will be covered by these guidelines;
   a) Email
   b) Internet
   c) Device Use
   d) Social Media

2. These guidelines are aimed at determining the broad RISE Trust principles regarding acceptable use and may be appropriately support by local use documentation for specific system use.

Email

3. Any communications using these systems represent The RISE 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 standard business communications.

4. Subject to the provisions set out in Section 10, Personal Use, you are not allowed to use the systems other than for genuine business 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 RISE Trust Disciplinary Procedure. The RISE Trust retains the right to remove access to these facilities if misuse or misconduct occurs.

5. 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.

6. 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

7. E-mails and other electronic communications have the same status as any other RISE Trust record and are to be treated in accordance with all associated RISE Trust policies. Such communications, where they are kept as a RISE 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.

8. No e-mail or other electronic transmission should be retained for longer than 12 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.

9. All users must therefore be familiar with The RISE Trust Records Management and Retention of Records Policies and act in accordance with the standards outlined in these documents.

Email Etiquette

10. In promoting good practice, The RISE 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 RISE Trust and mitigate risks.

There are many etiquette rules, and these will differ according to the nature of the user's business but outlined below are some rules that The RISE Trust recommends.

a) System Use

1. It is RISE Trust policy that e-mails should be read on a regular basis and all correspondence is to be dealt with at least to the standards outlined in this document and associated policies (see paragraph 77)
2. During any absence, arrangements are to be made that ensure messages can be diverted to a suitably authorised manager.
3. Use Outlook Out of Office.
4. Consider whether e-mail is the most appropriate method for communication.
5. Do not impersonate any other person when using e-mail.
6. Do not access a web site direct from an e-mail link.
7. Do not create mail congestion by sending trivial messages to users.
8. Users are to be cautious when accepting e-mails – it is not difficult to fake both content and sender.
9. 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

1. Be concise and to the point.
2. Answer all the questions and pre-empt further questions.
3. Make it personal.
4. Use templates for frequently used replies.
5. Keep to the message thread.
6. Use a meaningful subject.
7. Be polite.
8. Use appropriate language.

c) Style, Tone and Format

1. Font should be Century gothic, style Regular, size 12 and black in colour except where otherwise required by the recipient.
2. Background should be white rather than any other colour or personalisation of the page.
3. Use proper spelling, grammar and punctuation.
4. Use The RISE Trust structure and layout including the mission statement
5. Do not write in CAPITALS – it could be construed as shouting.
6. Consider the appropriateness of the use of acronyms, abbreviations and emoticons.
7. Be careful with formatting and comply with The RISE Trust Accessible Format Policy or best practice.
8. Use active rather than passive language.
9. Avoid long sentences and consider the length of the e-mail.
10. Do not send or forward e-mails or attachments with prohibited material.
12. Consider the wording used upon starting and ending the e-mail.
13. Adopt signatures that include RISE Trust name, job function, telephone, working hours, mission statement and address – CEO distributes example.
14. Avoid sending confidential, sensitive or personal information by e-mail.
15. Never send confidential messages by e-mail without getting the recipients agreement.

d) Options

1. Do not overuse the high priority option.
2. Ensure that the e-mail has The RISE Trust disclaimer.
3. Do not overuse the Reply to All.
4. Do not overuse Group or All Mail User options.
5. Use the cc field sparingly, considering carefully the need for others to receive it.
6. Do not print out e-mails without considering the need for a hard copy.

e) Replies

1. Answer swiftly and in accordance with RISE Trust expectations ie: checking emails daily and acknowledging receipt of emails within 48 working hours
2. RISE Trust staff must use their out of office notice if non-working day or on annual leave
3. Do not forward chain, pyramid or similar schemed e-mails.

4. Do not copy an e-mail or attachment without careful consideration of need.
5. Do not forward virus hoaxes but do inform the Information Security Office or IT provider of receipt.
6. Do not reply to unsolicited bulk e-mail, known as spam.
7. Do not abuse others, even in response to abusive e-mails received.
8. In a reply - state clearly what is required of the recipient.
9. When replying do not 'reply all' unless necessary.
10. If a recipient asks you to stop sending them personal messages then always stop immediately.

f) Attachments

1. Do not attach unnecessary files.
2. Use links in e-mails wherever possible.
3. Never open an e-mail attachment from an unexpected or untrustworthy source – if in doubt check with CEO and/or Oakford Technology Ltd

g) Before Sending

1. Read the e-mail again carefully and consider the content.
2. Consider how the recipient will interpret the message and ensure your intention is clear.
3. Imagine that you are talking to them face to face.
4. Retain copies of important e-mails, bearing in mind RISE Trust policy on records retention.
5. Ensure that the address is correct, particularly when using autofill, if using Bcc ensure that it correctly completed. *This is the largest cause of data breaches therefore at The RISE Trust we pay very close attention to this point.*

h) Deleting e-mails

1. 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
2. To be completely sure an e-mail is deleted you must then use the toolbar ('folder' tab) to access the option 'Recover deleted items'
3. 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 RISE Trust in any adverse manner, and 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 RISE 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 RISE 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 RISE Trust in terms of:

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

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

Device Use

Laptop, Mobile Phone and iPad

15. Any communications using these systems represent The RISE Trust inc texts, WhatsApp, FaceBook Messenger. Therefore, users should ensure that all messages and communications created are professional in tone, content and branding. 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. Where possible notifications will be turned off.

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. All phones should ideally be stored away whilst driving and any messages retrieved at the end of the journey when it is safe to do so. The RISE promotes use of the 'Do not Disturb I'm driving' setting.

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 6 digit 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) – when changing PIN please notify Kirsti Turner of changes

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 000000 when returning the phone or a sticker with the PIN code attached to the phone.

Device Use Security

26. When making use of these systems users must ensure that user IDs and passwords 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 RISE Trust equipment. Where the items are portable and of higher risk of theft, i.e. mobile phones or laptops, basic steps must be taken, i.e.

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. Secure the phone and laptop at home as if is a personal possession. Do not lend the phone or laptop to anyone else. The RISE Trust encourages staff to switch off if out of hours and at home.

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

31. Two factor authentication is installed on RISE accounts so if a new device is being used to access RISE system this will automatically be requested

32. Please refer to The RISE Trust Information Technology Policy, or senior management for further details. Advice and support is also available from The RISE Trust DPO.

Device Use Scanning of Documents

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

a) Scans done via 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.
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)

34. Any documents scanned via an 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.

35. Any documents scanned via an MFD must be scanned to email. Any new MFD's within The RISE 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 The RISE Trust SharePoint. 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. Any document with two or more items of PII data must be password protected when scanning.

36. Once the scanned document has been saved to The RISE Trust SharePoint the email containing the scanned document must be deleted.

Networked Devices

37. Any correspondence, photographs, drawings and/or plans scanned via a network scanner must be scanned as a PDF. All scanned files but must be converted to a PDF file before making them public.

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

39. 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

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

41. 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

42. The original source document should generally be destroyed/ shredded after it has been scanned, to avoid duplication and minimise administration. However, in exceptional cases there may be business 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 or DPO.

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

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

45. 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

46. 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:

1. Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved;

a) By the production of that document, or

b) 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.

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

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

a) 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.

49. 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.

50. 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 in order to achieve best practice, and therefore the legal admissibility of electronic documents.

51. 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 The RISE Trust Devices and Communication Methods

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

53. Personal use of The RISE 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.

54. 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 RISE Trust business commitments, adversely affect RISE Trust systems or harm The RISE Trust reputation;
c) It does not incur any additional expense to The RISE Trust; where it does, i.e. where The RISE Trust is liable for calls and text charges which relate to personal use then these costs must be reimbursed to The RISE 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 11 Prohibited Use;
f) They accept that usage is at their own risk and that The RISE 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 their own and not The RISE 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 The RISE Trust. This e-mail is the personal responsibility of the sender"

h) They do not use The RISE 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 RISE Trust e-mail address for this purpose is to be accompanied by a disclaimer as outlined above.

55. Personal e-mails blocked by The RISE Trust content filtering routines will not be released to the recipient. The RISE 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.

56. 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.

57. 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.

58. Any complaints or allegations of misuse and misconduct may be dealt with in accordance with The RISE Trust Disciplinary Procedure.

Prohibited Use

59. Every user must ensure that all electronic communications activities are not illegal, inappropriate nor contrary to the good conduct of The RISE Trust business. In order to ensure compliance, it is The RISE Trust policy to prohibit certain activities. In particular users must not use The RISE 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 RISE Trust Policies. These include, but are not limited to, The RISE Trust Equal Opportunities, 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) Open any e-mails which do not appear to be related to The RISE Trust business and seem to contain jokes, graphics, or images as such e-mails regularly contain viruses, or
e) Play computer games.

60. Any complaints or allegations of misuse and misconduct may be dealt with in accordance with The RISE Trust Disciplinary Procedure.

61. The following section provides more detailed guidance on what The RISE 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 RISE 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

62. The use of RISE 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 RISE Trust software has accessed the web page might embarrass The RISE Trust if made public, then it may not be viewed.

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

64. The RISE 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

65. 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.

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

Computer Misuse

67. It is forbidden to use The RISE 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.

68. Protective measures against computer malicious programs (malware) have been taken by The RISE 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

69. The RISE 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.

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

71. Document downloads are permissible, but as such must comply with legislative requirements and are subject to The RISE Trust filtering routines.

Impersonation

72. 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 RISE 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 The RISE Trust policy.

73. If users are in doubt as to the appropriateness of material they are accessing or if they are receiving inappropriate/ offensive communications and material, they must inform a RISE Senior manager as soon as possible.

74. Any complaints or allegations of misuse and misconduct may be dealt with in accordance with The RISE Trust Disciplinary Procedure.

Contracts

75. The RISE 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 RISE Trust Purchasing Card.

Social Media

76. 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 and Instagram
b) Online discussion forums, such as Ning
c) Collaborative spaces, such as Wetpaint
d) Media sharing services, such as Flickr and YouTube
e) Blogs, (personal Web Logs), such as Blogger
f) Microblogging applications, such Twitter.

77. 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 RISE Trust reputation.

78. 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/ 2018
c) Freedom of Information Act 2000
d) Safeguarding Vulnerable Groups Act 2006
e) The RISE Trust Equal Opportunities Policy
f) The RISE Trust Confidentiality and Information Sharing policy
g) The RISE Trust Information Technology Policy

Authorised Users of Social Media

79. Use of social media, on behalf of The RISE Trust, is to be used only by:

a) Those people who have been identified as media spokespeople with the agreement of the relevant senior manager and the CEO where applicable;

b) Other users who have a specifically defined role, have had a business case approved and also 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 situation.

80. For those people authorised to respond on behalf of The RISE 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.

81. Staff authorised to speak on behalf of The RISE 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 section 13.5

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

Using Social Media on Behalf of The RISE Trust

83. Social media, on behalf of The RISE 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 RISE 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 RISE Trust users in breach of RISE Trust codes of conduct or policies;

f) Breach The RISE Trust misconduct, equal opportunities or bullying and harassment policies.

g) To release information that could be considered confidential; or

h) Damage The RISE Trust reputation.

Correct Use of Social Media for The RISE Trust Business

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

85. 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 RISE Trust purposes. To assist with this, all users must adhere to the following requirements:

a) All links should be to The RISE Trust website or other approved sites;
b) The therisetrust.org email address should be used for official RISE Trust purposes, unless otherwise agreed by the relevant RISE Trust Senior Manager;
c) The use of The RISE Trust logo and other branding elements should be used where appropriate to indicate The RISE Trust support or where The RISE Trust responds formally;
d) The logo should not be used on social media applications which are unrelated to or are not representative of The RISE Trust official position;
e) Staff representing The RISE 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 RISE Trust officers acting on behalf of The RISE Trust to deceive, even inadvertently, others users of social media;
f) They should ensure that any contributions they make are professional and uphold the reputation of The RISE Trust; Ensure all contributions are factual and compliant with RISE associated guidelines originated from appropriate sources such as NHS, Change for Life etc.
g) Comply with all the relevant legislation and The RISE Trust policies on IT;
h) They must not promote or comment on political matters or issues that may be regarded as such; and
i) Avoid endorsements that are not relevant to the operation The RISE Trust;
j) Be aware that all information that you post on behalf of The RISE Trust may be subject to the Freedom of Information Act

Using Social Media in a Private and Personal Capacity

86. The RISE 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 RISE Trust.

87. 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 RISE Trust also routinely monitors comments made about it, in social media.

88. Unless staff are authorised to speak on behalf of The RISE 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 RISE Trust;
b) Avoid any actions that would put RISE Trust users in breach of The RISE Trust codes of conduct or policies;
c) Avoid publishing or passing on links to any defamatory and/or knowingly false material about The RISE 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 RISE Trust misconduct, equal opportunities or bullying and harassment policies;
e) Not reveal confidential information relating to his/her employment within The RISE Trust; and
f) Not say anything that would damage The RISE Trust reputation. *Report any defamatory material observed on social media to management immediately.*

Cyberbullying

89. Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

90. Prevention activities are key to ensuring that adults are protected from the potential threat of cyberbullying. All adults are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

91. If cyberbullying does take place, records should be kept of the abuse such as text, e-mails, website or instant messages and texts or e-mails should not be deleted. Adults are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

92. Adults may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process.

93. Adults are encouraged to report all incidents of cyberbullying to their line manager. All such incidents should be taken seriously and dealt with

in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

94. Equally Adults need to be very clear that any online activity they undertake that may be considered bullying of another person, whether child or adult, or any threatening statements will be considered a disciplinary matter and may lead to criminal investigation and conviction. This is regardless of whether the behaviour has occurred within or outside of work, on work or personal equipment.

Other Guidelines

95. 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. In particular 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 RISE 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

965. 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.

97. 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.

Use of video calling

98. The RISE Trust will use WhatsApp, FaceTime for individual video calling only. Microsoft Teams (as advised by our DPO) will be used for group calls both within and outside of the organisation.

99. When using Microsoft Teams – please be aware of what is behind you and blur it if you are uncertain of the confidentiality of the information in the background.

100. All RISE staff will follow the Virtual etiquette when using video calls

Breaches of this Policy

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

102. If it is believed that The RISE Trust has been brought into disrepute this may constitute misconduct or gross misconduct and disciplinary action will be applied as appropriate.

Link with other policies

103. This document should be read in conjunction with these policies:

- ICT policy
- Disciplinary Policy and Procedures
- Equal Opportunities Policy
- Code of Conduct
- Data Protection Policy (GDPR) 2019
- Harrassment and Anti-bullying Policy
- Confidentiality
- IT
- Virtual etiquette

104. All adults must adhere to and apply the principles of this document in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

Appendix B – Relevant legislation *(from WSCB Social Networking policy)*

Adults should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer misuse act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data protection Act 2018

This protects the rights and privacy of individual's data. It makes our data protection laws fit for the digital age in which an ever-increasing amount of data is being processed. Empowers people to take control of their data. Supports UK businesses and organisations through the change. Ensures that the UK is prepared for the future after we have left the EU.

Our organisation aims to ensure that all personal data collected about staff, children, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format (see The RISE Trust Data protection Policy March 2019).

Effective data protection relies on The RISE Trust adequately protecting their IT systems from malicious interference. In implementing the GDPR standards, the Act requires the Trust handles personal data to evaluate the risks of processing such data and implement appropriate measures to mitigate those risks.

Freedom of information act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications act 2003 (superseded The Telecommunications Act 1984)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious communications act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of investigatory powers act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks act 1994
This provides protection for Registered Trademarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, designs and patents act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their

reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Criminal justice & public order act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and religious hatred act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from harassment act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of children act 1978 (1999 Dept Of Health Draft)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise).

Sexual offences act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals fall in this

category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public order act 1986 (amendment 1996)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene publications act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human rights act 1998 (amendment 2005)
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The organisation is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.