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**
Revision Due	**February 2027**

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
5	February 2026	Updated according to OneWest master policy - all staff and trustees to acknowledge receipt

THE RISE TRUST

1. Introduction

Data, information and networks and services are vital to The RISE Trust. Without good use of these assets The RISE Trust would be unable to provide effective and efficient services to children, young people and support parents. Hence an understanding of what is expected while using these assets will help individuals protect themselves and their colleagues and The RISE Trust's networks and services and the data processed therein and ultimately protect The RISE Trust's reputation.

This Acceptable Use Policy (AUP) aims to provide clarity on the behaviours expected and required by The RISE Trust staff, service providers and contractors to protect all users of data and equipment and minimise risk. It is a framework on how to conduct The RISE Trust business to meet legal, contractual and regulatory requirements and defines how individuals must behave to comply with this policy.

2. Scope

All trust equipment (all information systems, hardware, software and channels of communication, including voice- telephony, social media, video, email, instant messaging, internet and intranet) are within the scope of this policy. User's personal information which is processed by the trust's equipment and services is also in scope.

Users are defined as all members of staff (full-time and part-time), temporary members of staff, volunteers, trustees and contractors, and any other person or organisation acting for or on behalf of The RISE Trust, that have been granted access to The RISE Trust systems and data to perform a specified function / role.

All users must make themselves familiar with and comply with the guidelines at each of the appendices of this policy.

3. General Principles

These general principles apply to user's use of trust equipment and services:

- Users agree to comply with this AUP and confirm that they understand that any breach of this policy may result in disciplinary action being taken.
- Users are responsible for their own actions and that they act responsibly and professionally, following the trust standards of behaviour and respect The RISE Trust, colleagues, partners, children, young people and parents.
- Users use the most efficient, effective and secure communication tools to fulfil their roles.
- All equipment and services provided by the trust are primarily for business use.
- Although the occasional use of equipment and services for personal reasons is permitted, its use for these reasons must not be excessive, inappropriate or interfere with carrying out any responsibilities and not adversely affect either The RISE Trust's business or reputation or place The RISE Trust at unnecessary risk.
- Use of information, systems and equipment is in line with The RISE Trust's security and information management policies.
- Do not use the trust equipment and services to send prohibited material that includes 'spam and unsolicited messages', 'false or misleading information', 'copyrighted material', 'illegal content or offensive material'.
- Any breach of this AUP is reported to their line manager and official procedures are followed when a breach of personal data is suspected or reported.
- Understand that they can whistle blow / raise a concern if they believe that someone is misusing trust assets, information or electronic equipment.
- Never undertake illegal activity, or any activity that would be harmful to The RISE Trust's reputation or jeopardise staff and/or data that is processed on trust technology.
- Understand that both business and personal use of trust systems will be monitored as appropriate.
- Users' can have no expectation of privacy for anything that is created, stored, sent or received via The RISE Trust systems.

- Should either non-compliance with this policy and guidelines or an intentional breach of this policy be discovered, senior management shall have the authority to take immediate steps as considered necessary, including disciplinary action.
- User should complete all training and awareness courses related to the use of trust networks and services made available to them, including data protection and cyber security courses, to make best use of equipment and services and support the understanding, recognition and reporting of threats, risks, vulnerabilities and incidents.

4. Key concepts

4.1 Security of assets

Users are responsible for the day-to-day security of trust equipment and hence they must:

- Comply with The RISE Trust's Security Policy and Information Security Policy.
- Keep all portable devices that are of higher risk of theft, i.e. mobile phones or laptops, safe and secure and immediately report any loss or damage of their equipment to their line manager and log a security incident. If the device is a RISE Trust work phone/smart phone, users must contact the CEO urgently to ask for the phone to be suspended.
- While at in the office, store the phone/laptop and associated equipment with due care. Do not leave a phone unattended on a desk and ensure your laptop is secured overnight.
- If a Trust device is taken home secure them as if is a personal possession. Do not lend the phone or laptop to anyone else.
- Protect Trust equipment appropriately when travelling, for example:
  - Laptops must always be carried as hand luggage in a lockable case
  - Never leave a portable device visible in parked vehicles
  - Never leave equipment unattended in a public place, for example on public transport
  - Return all trust assets when leaving The RISE Trust. Failure to return equipment could lead to steps being taken to recover the cost, which could include legal action through the civil courts. Line Managers must complete all appropriate exit procedures with leavers.

Proven breaches of these security requirements, which are defined in The RISE Trust Information Security Policy, may lead to action being taken under The RSE Trust Disciplinary Procedure.

4.2 User IDs and passwords

Users must:

- Protect usernames, staff numbers, and passwords appropriately.
- Create secure passwords in accordance with the Trust's Information Security Policy.
- Passwords must not be stored in shared folders or written down.
- Not log on to any trust systems or services using another user's credentials.
- Lock a device / screen when leaving a system or service for short periods, such as taking a break during a working day.
- Log out /shut down all trust systems and services connected to the trust internal network during non-working hours, such as at the end of the working day.

4.3 Unacceptable use of systems and services

Every user of the trust's systems and services must ensure that all electronic communications activities are not illegal, inappropriate nor contrary to the good conduct of The RISE Trust business. To ensure compliance it is trust policy to prohibit certain activities. Users must not use The RISE Trust systems and services to:

- Create, review or transmit material that is inappropriate, offensive, untrue, defamatory, malicious, discriminatory, racist, disruptive, harassing or threatening in nature.
- Spread gossip, send chain mail letters, or copy or send material in breach of copyright.
- Download programs or any other software from the Internet.
- Create, review or transmit jokes, stories or cartoons.
- 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
- Play computer games.

Although The RISE Trust acknowledges that users are often unable to control the flow of emails and Internet transmissions / webpages, users have a responsibility to ensure that inappropriate or offensive communications are deleted from systems and services. End use devices, such as laptops can be used and screens viewed by anyone, so it is essential that users are aware of their roles and responsibilities in terms of use of trust systems and services and comply with this AUP.

Any complaints or allegations of misuse and misconduct may be dealt with in accordance with The RISE Trust's disciplinary procedure.

Appendix One provides further details of what The RISE Trust deems to be unacceptable use of electronic communications, systems and services.

4.4 Procurement

The RISE Trust has detailed procedures to be followed when procuring electronic communications, systems and services relating to both teaching and administration. Security of systems and services and the data managed by them is a crucial aspect of the procurement of electronic communications, systems and services.

Goods and services may be purchased via The RISE Trust systems and services. Where any goods/services are purchased over the Internet consideration should be given to only using a RISE trust bank Card which provides financial protection and assurances.

5. 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

Appendix One – Unacceptable use of electronic communications, systems and services

Appendix One provides definitions of key terms and describes some key concepts relating to the use of the trust systems and services.

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 RISE Trust CEO as soon as possible.

It is repeated that any complaints or allegations of misuse and misconduct may be dealt with in accordance with The RISE Trust Disciplinary Procedure.

Definitions

The following definitions apply to this AUP and related trust policies.

Defamation.

Defamation is defined as 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 UK legislation. Hence it is prohibited to transmit send, access or transfer information or messages whose content or intent would reasonably be considered to be abusive, disrespectful, hurtful or undermining in nature using trust systems and services. The communication of information regarding alleged professional and/or personal misconduct is also to be avoided.

Discrimination and Harassment.

Discrimination and harassment is defined as 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.

Harassment.

Harassment is defined as the 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

The use of The 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 restriction 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.

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

The RISE Trust will not discuss 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

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 emails and to employ cut and paste techniques. Hence care should be taken when using these techniques. Individuals should be aware that non-compliance with the Act may result in prosecution through the courts.

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

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:

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

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

The RISE Trust has adopted a standard set up for all laptops so that all software is correctly installed and properly licensed. It is prohibited to download programs or any other software.

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.

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

Impersonation

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.

Appendix Two – Email – Principles and Guidelines

Principles

The trust email system is the primary communications system. All the general principles described in this AUP apply to the use of The RISE Trust's email system, but the following points are stressed:

- Any correspondence using email represents The RISE Trust.
- You should ensure that all email messages sent 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 RISE Trust's communications policy.
- Care must be applied prior to the release of any email, 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 emails 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.
- Copying ('Cc' and 'Bcc') emails to correspondents should be kept to a minimum.
- Confirmation of receipt should be obtained for important email messages.
- The unnecessary inclusion of attachments, particularly added to messages sent internally, is also discouraged.

Email messages have the same status as any other trust record and are to be treated in accordance with all associated trust policies relating to topics, such as data protection and safeguarding etc. Correspondence is likely to be eligible for disclosure in response to a request for access to information under current legislation, such as the Data Protection Act 2018 and/or Freedom of Information Act 2000.

No email or other electronic transmission should be retained for longer than 12 months unless:

- It is classified a trust record and in which case its retention must comply with The RISE Trust's Retention Policy.
- There is a clear business need for retention.

Hence all users must familiarise themselves with The RISE Trust's Record Management and Retention Policy.

Guidelines

To get the most out of email – be professional, efficient and protect yourself and The RISE Trust - users should follow these guidelines that draw-on principles and best practice:

Sending email

Before deciding to send an email you should:

- Consider whether email is the most appropriate/suitable method for communication.
- Do not congest the email system by sending trivial messages to users.
- Do not impersonate any other person when using e-mail.

In terms of the content of your emails you should:

- Pick a meaningful subject.
- Be concise.
- Answer all questions and try to pre-empt further questions.
- Make it personal.
- Keep to the message thread.
- Use templates for frequently used replies.

In terms of the style, tone and format of your emails they should:

- Unless instructed otherwise, use The RISE Trust's standard font – Century Gothic
- Use a proper structure and layout.
- Comply with The RISE Trust's policy covering accessibility
- Use proper spelling, grammar and punctuation.
- Use active voice rather than passive voice language.
- Avoid long sentences and consider the length of the email.
- Do not write in CAPITALS – use of capital letters throughout an email or in sections could be construed as 'shouting'.
- Keep your language gender neutral.
- Consider the wording used upon starting and ending the e-mail.
- Use The RISE Trust approved signature block that should include your name, details of job/role, telephone number and email address.
- Avoid sending confidential, sensitive or personal information by e-mail.
- Never send confidential messages by e-mail without getting the recipients agreement.
- Do not send or forward emails or attachments with prohibited material.

Consider the following options when writing an email:

- Do not overuse the high priority option.
- Use the 'Cc' field sparingly by considering the need for others to receive your email.
- Always use the 'Bcc' (Blind Carbon Copy) field when emailing multiple external recipients (for example parents). This will ensure recipients cannot see each other's email addresses.
- Ensure that the e-mail has The RISE Trust disclaimer.
- Do not overuse the 'Reply to All' feature.
- Do not overuse 'Group' or 'All Mail User' options.
- Do not print out e-mails without considering the need for a hard copy.

And follow these instructions relating to attachments.

- Do not attach unnecessary files.
- Wherever possible send links to documents held in The RISE Trust SharePoint rather than send an attachment.
- Check that an attachment does not include any information which should not be disclosed. For example, a master form has been over-saved with personal information.
- Never open an e-mail attachment from an unexpected or untrustworthy source.

Finally, before sending an email:

- Check that the email address is correct, particularly when using the 'auto-fill' feature. If using the 'Bcc' field, ensure that it is completed correctly. This is the largest cause of data breaches in The RISE Trust. Hence pay very close attention to this point.
- Re-read the email carefully and consider the content before sending.
- Imagine that you are talking directly to the recipient.
- Consider how the recipient will interpret the message and ensure your intention is clear.
- Consider delaying the release of your email. In some email clients such as MS Outlook, you can delay the delivery of an individual message by having it held in the **Outbox** for a specified time after you click **Send**.

If you are satisfied after you have checked a draft email, then click **Send**.

Importantly, retain copies of important e-mails in accordance with The RISE Trust's information management policy and retention policy.

Managing your Inbox

Managing your Inbox/es efficiently and effectively is important. Delayed responses to requests / instructions in emails could have significant impact on the day-to-day business of the trust and may undermine the reputation of the trust. Hence, it is important that your Inbox is monitored and well managed by doing the following:

- Checking regularly for any emails and responding to / dealing with them in accordance with The RISE Trust's respond within three working days.
- Be cautious when reading and responding to emails – it is not difficult to fake both content and sender.
- Users should check that the content provides reasonable assurance of its authenticity and should consider checking by alternate means that it has come from the sender.
- Do not access a web site direct from an e-mail link. Instead copy and paste a link into a website into a browser first.
- For any periods of absence use the 'out of office' message feature to notify correspondents of your absence and notify them when you will return to work

and what will happen to their email until your return to work. Include any alternative arrangements for dealing with emails where appropriate.

- For extend periods of absence consider diverting your Inbox to a suitably qualified co-worker or your manager.

Replying to emails

In responding to / replying to emails you should:

- Answer them swiftly and in accordance with The RISE Trust standards (3 working days).
- Do not forward chain, pyramid or similar schemed emails.
- Do not copy an e-mail or attachment without careful consideration of need to do so.
- Do not forward virus hoaxes. Instead inform The RISE Trust's information security lead and/or the IT Department first.
- Do not reply to unsolicited bulk e-mail, that is known as spam.
- Do not abuse others, even in response to abusive e-mails from them.
- In a reply state clearly, what is required of the recipient.
- If a recipient asks you to stop sending them personal messages, then always stop immediately.

Deleting e-mails

Unless there is a clear need to do otherwise emails should be deleted after they have been actioned. Where there is a need to retain an email or email thread as a record it should be copied to the appropriate file store for retention as soon as possible and then deleted from the email system. The RISE Trust's email system should not be used as a file store.

Key tasks to do when deleting emails:

- 'Double delete' an email/s as a minimum. This means that after deleting an email/s you must access the deleted items folder and delete them again.
- To be completely sure an e-mail is deleted you must then use the toolbar to access the option 'Recover deleted items'
- 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.

Appendix Three - Internet Use

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

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 this AUP. 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.

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:

- loss of productivity.
- impact on network resources.
- security issues.
- legal liability.
- adverse publicity.

Appendix Four – Device use – Mobile phone and tablet

Principles

Staff communicating with parents/carers, third-party suppliers and external organisation/s with trust devices represent The RISE 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 email guidelines above for some hints and tips.

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.

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.

Staff must not use mobile phones in any manner that may put them, other staff, children/young people or members of the public at risk. All personal phones should be put away during sessions and only RISE Trust phones used for calls, photos, etc.

Guidelines

Appendix Five – Device use – Scanning Documents

Principles

The principles must be followed when scanning original documentation:

- Ideally all documents that are scanned using either a Multi-Function Device (MFD) or a stand-alone scanner must be scanned and saved as a PDF and then transferred immediately to The RISE Trust SharePoint.
- Other file formats that are more suitable for storing a particular form of document, such as high-resolution photographs etc., may be used instead although before those documents are passed to external stakeholders, they should be converted to PDF.
- All relevant metadata, such as date and title, should be captured when the document is saved. No personal identifiable data should be included in the metadata.
- A scanned document must be checked against the original to ensure an accurate and complete copy.
- A scanned document must be managed in accordance with The RISE Trust Records Management and Retention Policy.

Guidelines

Multi Functioning Devices (MFD) - The RISE Trust photocopier

The following guidelines apply to the use of MFD:

- MFDs are set to save scanned documents as a PDF. This is the default setting and cannot be changed.
- MFDs in The RISE Trust are set as default to scan to a user's account that is denoted by their email address.
- Use of 'Scanned File' folders is not recommended due to and absence of access control to these folders.
- Once the document is scanned to the user's work email address, users must save the document to one of The RISE Trust's managed service, i.e.: SharePoint.
- Once the scanned document has been saved to SharePoint the file containing the scanned document should be deleted.

Stand-alone devices

The following guidelines apply to the use of Stand-alone devices:

- Any documents scanned via a stand-alone device must be scanned as a PDF.
- 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 (metadata) and wherever possible a unique identifier. No personal identifiable data should be used in the document title.

Original documents

The following guidelines apply to the original documents once they have been scanned:

- The original document should generally be destroyed after it has been scanned, to avoid duplication and minimise administration. However, in exceptional cases there may be reason/s why the document should be retained. If in doubt as to whether an original document should be kept, users should consult the Records Management and Retention Policy, the CEO or the DPO.
- Thereafter the original document must be managed in accordance with Records Management and Retention Schedules.
- All scanned documents must be checked to ensure the scanned image is an accurate and complete copy of the original source document.

Whether a document is scanned via any of the methods detailed, any further transfer of the document must be done considering the sensitivity and confidentiality of the contents of the document.

Scanned Documents and Legal Compliance

It is important to be aware that scanned documentation may be used in legal cases, and the following describes the standing of scanned documentation under various legislation.

Admissibility - 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.

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

Admissibility - 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.*

Ultimately an original document will always hold more weight than a copy. 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.

Admissibility – British Standard of scanned documents

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

Copyright

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.

Appendix Six – Device Use – Personal Use of The RISE Trust Devices and Communication Methods

The hardware, software and materials relating to electronic communications are owned wholly by The RISE Trust, which provides access to them to facilitate effective business communication within the workplace. As such they are provided primarily for business use.

Personal use of The RISE Trust mobile phones or systems to browse the Internet or send emails is not permitted, however staff are allowed use of personal phones during breaks/ lunch times only. Excessive use of personal phones will be dealt with as a disciplinary issue.

In exceptional circumstances, personal use of trust 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. staff need to unexpectedly work late. There is no expectation that such calls should be paid for by the individual.

You must not use The RISE Trust facilities for any for-profit business or commercial gain.

.

Appendix Seven - Social Media

Introduction

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:

- Social networking utilities, such as Facebook, Instagram, X (formerly Twitter)
- Online discussion forums.
- Collaborative spaces
- Media sharing services, such as Flickr and YouTube
- Blogs, (personal Web Logs), such as Blogger
- Microblogging applications, such X, Bluesky and Reddit.

It is important that everyone uses the technologies and services effectively, flexibly and in an appropriate manner. While at work and at home users must act in a way that does not compromise The RISE Trust's reputation.

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:

- Copyright, Designs & Patents Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- The RISE Trust Equality, Diversity and Inclusion Policy (EDI)

Principles

When using social media in a private and personal capacity users should also follow the principles suggested by the social media sites for their own safety. These can normally be found on the information pages of each social media site. Those general guidelines include:

- Taking care how users are perceived, as the boundaries between their professional life and private life can become blurred in social networks.
- Considering whether users would be happy for their colleagues, managers or service users to read the comments, and consider what their reaction might be.
- Showing respect for others. You should be respectful of The RISE Trust and your fellow staff and volunteers.
- Ensuring that the privacy of others is always respected.
- Obtain the permission of individuals before posting contact details or pictures.
- Not use sites for accessing or sharing illegal content; and
- Use social media in a responsible fashion and avoid giving out personal information about you or your family.

Guidelines

Authorised users of social media

Social media is to be used on behalf of The RISE Trust only by:

- Those people who have been identified as media spokespeople by the CEO or Deputy CEO.

- Those with another defined role that have been appropriately trained. These roles should be defined in a business case that is supported by a member of the senior leadership team / head of department.
- Users who have been given responsibility as part of managing an emergency.

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.

Where authorised individuals from key partners and/or external organisations are authorised to act on behalf of The RISE Trust, they will also be expected to comply with all relevant trust policies and associated guidelines.

Staff authorised to speak on behalf of The RISE Trust should ensure that they comply with set out in the next section 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 appropriate section below.

Access to social media sites

Social media sites are made available subject to approval when using The RISE Trust iPads, iPhones and laptops.

Restrictions on the use of social media

While using social media on behalf of The RISE Trust, users must not:

- Publish any content that 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.
- Be used for party political purposes or specific campaigning purposes.
- Be used for the promotion of personal financial interests, commercial ventures, or personal campaigns.
- Be used in an abusive or hateful manner.
- Be used for actions that would put The RISE Trust users in breach of trust codes of conduct or policies.
- Breach The RISE Trust misconduct, EDI or bullying and harassment policies.
- To release information that could be considered confidential; or
- Damage The RISE Trust reputation.

Correct use of social media for The RISE Trust business

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

- All links should be to The RISE Trust website or other approved sites.
- The RISE Trust domain email address should be used for official trust purposes, unless otherwise agreed by the relevant senior manager.
- 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.
- The logo should not be used on social media applications which are unrelated to or are not representative of The RISE Trust official position.
- 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 The RISE Trust staff/

trustees acting on behalf of The RISE Trust to deceive, even inadvertently, other users of social media.

- They should ensure that any contributions they make are professional and uphold the reputation of The RISE Trust.
- Comply with all the relevant legislation and The RISE Trust policies on IT.
- They must not promote or comment on political matters or issues that may be regarded as such.
- Avoid endorsements that are not relevant to the operation The RISE Trust.
- 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

The RISE Trust understands that staff may use social media, on their own equipment in their own time, for their own private use. 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.

These guidelines do not mean that staff can never post comments on these websites about their work for The RISE Trust. The trust routinely monitors comments made about it, in social media.

Staff must not connect with current children/ young people on personal social media. Staff may wish to mask or edit their username to hinder children/ young people locating them on social media platforms. For more information see The RISE Trust IT and Safeguarding Policies.

Unless staff are authorised to speak on behalf of The RISE Trust, outside of their work time they should:

- Use a disclaimer to make it clear that their views are their own and not necessarily those of The RISE Trust.
- Avoid any actions that would The RISE Trust users in breach of The RISE Trust codes of conduct or policies.
- Avoid publishing or passing on links to any defamatory and/or knowingly false material about The RISE Trust, your colleagues and/or customers
- Avoid using language that could be deemed offensive to others.
- Not breach The RISE Trust misconduct, equal opportunities or bullying and harassment policies.
- Not reveal confidential information relating to his/her employment within The RISE Trust.
- Not say anything that would damage The RISE Trust’s reputation.

Using social media in connection with vulnerable people

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.

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 these guidelines

The RISE Trust takes appropriate and safe use of social media very seriously and any breach of this policy could lead to disciplinary action.

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.