Rutland
County Council

RUTLAND ADULT LEARNING AND SKILLS SERVICE

E safety Policy

Scope of the Policy

This policy applies to all members of Rutland Adult Learning and Skills Service *(RALSS)* community (including staff, learners volunteers, visitors, community users) who have access to and are users of RALSS ICT systems, both in and out of the *RALSS.*

The Education and Inspections Act 2006 empowers leaders of institutions to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the RALSS site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of RALSS, but is linked to membership of RALSS. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

RALSS will deal with such incidents within this policy and associated behaviour and anti-bullying policies.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within RALSS.

Management Team

The Management Team are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Management Team has taken on the role of E-Safety Lead in conjunction as the Safeguarding Lead.

The role of the E-Safety Lead will include:

- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Management Team

Head of RALSS

- The RALSS Manager has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator / Officer.
- The RALSS Manager and should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The RALSS Manager is responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The RALSS Manager will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.

E-Safety Lead:

The Safeguarding / E Safety Co-ordinator will:

- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing RALSS e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority / relevant body
- liaise with RALSS technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments)
- reports regularly to Senior Leadership Team

RALSS Network Lead:

The Network Lead is responsible for ensuring:

- that the RALSS technical infrastructure is secure and is not open to misuse or malicious attack
- that RALSS meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported.
- that monitoring software / systems are implemented and updated.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the RALSS e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E Safety Lead for investigation / action / sanction
- all digital communications should be on a professional level and only carried out using official RALSS systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the e-safety and acceptable use policies
- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

E Safety / Safeguarding Designated Person

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Learners:

- are responsible for using RALSS digital technology systems in accordance with the RALSS Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

Community Users

Community Users who access RALSS VLE as part of the wider provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – leaners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in e-safety is therefore an essential part of the school's e-safety provision. Learners need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety action should be provided as part of Computing / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Learners should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit.

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand RALSS e-safety policy and Acceptable Use Agreements.
- The E-Safety Lead (or other nominated person) will receive regular updates through attendance at external training events or by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

Whilst RALSS has a managed ICT service provided by an outside contractor, it is the responsibility of RALSS to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of RALSS. It is also important that the managed service provider is fully aware of the RALSS E-Safety Policy / Acceptable Use Agreements.

RALSS will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices.
- All users will be provided with a username and secure password.
- A designated person is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- RALSS has provided enhanced / differentiated user-level filtering.
- RALSS technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. RALSS infrastructure and individual workstations are protected by up to date virus software.
- An agreed agreement is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) .

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by institutions of users bringing their own technologies in order to provide a greater freedom of choice and usability. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- RALSS has a set of clear expectations and responsibilities for all users
- RALSS adheres to the Data Protection Act principles
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by RALSS normal filtering systems, while being used on the premises

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow RALSS policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

RALSS will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

Social Media - Protecting Professional Identity

RALSS has a duty of care to provide a safe learning environment for pupils and staff. RALSS could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render RALSS liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

RALSS provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

RALSS staff should ensure that:

- No reference should be made in social media to learners
- They do not engage in online discussion on personal matters relating to members of RALSS
- Personal opinions should not be attributed to RALSS
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

RALSS use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

RALSS believes that the activities referred to in the following section would be inappropriate in a RALSS context and that users, as defined below, should not engage in these activities in school. RALSS policy restricts usage as follows:

User Actions

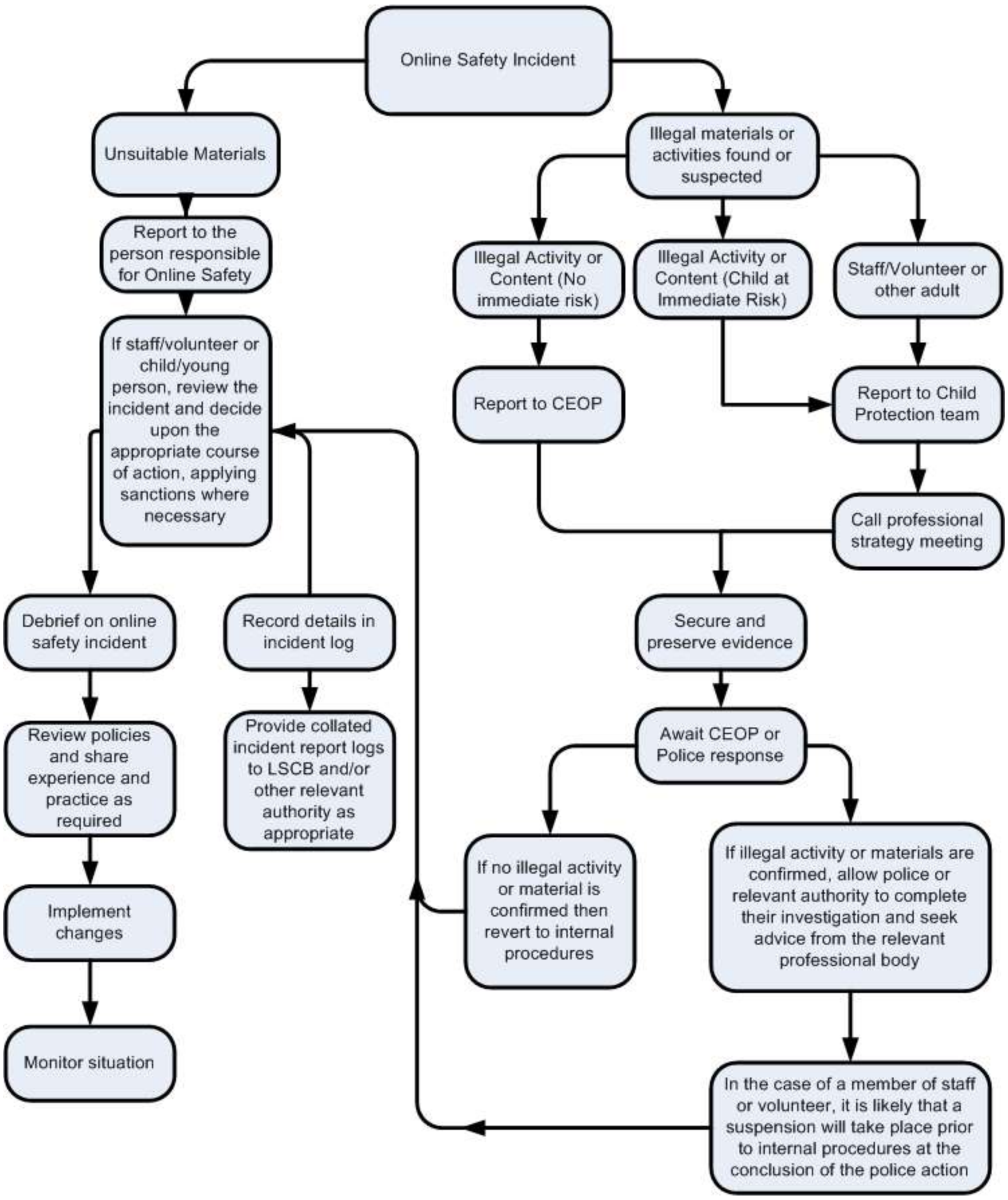
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using RALSS systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the RALSS will be responsible users of digital technologies, who understand and follow RALSS policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - criminally racist material
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for RALSS and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

RALSS Actions & Sanctions

It is more likely that RALSS will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Date	Reason for Review	Next Scheduled Review
October 2014	Updated as per two year cycle	August 2016
Aug 16	Scheduled Review	Aug 18

Owner: R Shore, Adult Learning Manager