E-Safety Policy
Including ICT Acceptable Use

Updated Date: September 2021

Approved By: Full Governing Body Date: October 2021

CONTENTS

PAGES

APPENDICES

Purpose of the Policy

- This policy sets out the expectations of E-Safety and Digital Responsibility at Reddish Vale High School and its approach in ensuring that all students are safe online and able to thrive in a positive learning environment.
- This policy applies to all members of the Reddish Vale High School community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of Reddish Vale ICT systems, both in and out of the school.
- The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of students when they are off the school 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 the school, but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action will be taken over issues covered by the published Behaviour Policy.
- Reddish Vale High School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.
- This policy should be read in conjunction with: the Behaviour and Anti-Bullying Policy and the Safeguarding Policy incorporating Child Protection Procedures.

Aims

- Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions about how to use technology as well as to feel able to report any concerns.
- All members of staff need to be aware of the importance of good technology practice in the classroom in order to educate and protect the children in their care.
- Plan to ensure that the whole school keeps abreast of new legislation and guidance in relation to E-Safety.
- Monitor, challenge, record and address effectively and appropriately any incidents arising with regard to E-Safety.

To achieve these aims

We will

1) Ensure that all stakeholders are consulted on the development, review, evaluation and impact of all relevant procedures and policies and are able to access these policies.

2) Ensure that all members of the school community have an understanding of E-Safety and are aware of the school's policy in relation to it.

3) Ensure that all staff are supported in knowing how to deal with incidents fairly and consistently should they arise.

4) Collect and analyse available information and data in relation to E-Safety incidents across the school.

5) Employ restorative approaches to encourage any students involved in inappropriate online behaviour to develop a greater understanding of the impact of their behaviour on others. Other parties including the school's pastoral managers, police liaison officer or any other agencies will be involved as appropriate.

6) Ensure that victims of E-Safety abuse are supported by employing strategies within school to challenge this behaviour and where appropriate enlisting the support of any other relevant agencies/professionals. Offer support or advice also to parents of students who are involved in or are victims of inappropriate online behaviour.

7) Ensure that any incidents of inappropriate online behaviour are recorded, monitored and addressed appropriately – information will be reported to other stakeholders.

8) Put a range of systems in place to actively encourage parents and all students across the school to report incidents of bullying and express their concerns in relation to it.

9) Ensure incidents are taken seriously, investigated thoroughly and acted on appropriately.

10) Employ systems to maintain a high standard of behaviour and respect for others throughout the school.

11) Be pro-active and put into place preventative strategies by raising awareness of standards and unacceptable behaviour towards others, inside school, in the community and online throughout the embedded curriculum, PSHE , the school's pastoral care system.

12) Ensure that any incidents reported with regard to inappropriate online behaviour between staff are dealt with in keeping with the school's disciplinary procedure.

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy.

We have a designated link Governor for Safeguarding which includes E-Safety.

The role of the Safeguarding Governor will include:

• termly meetings with the Designated Safeguarding Lead;

• reporting to relevant Governors / Board / committee / meeting.

Headteacher/Senior Leaders:

• have 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 Safeguarding Manager who will be supported by daily reporting from the IT Network Manager.

Safeguarding Manager/Designated Safeguarding Lead:

• should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of the school community. The Headteacher is responsible for ensuring that the Safeguarding Manager/IT Network Manager/Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant;

• will receive regular monitoring reports from the IT Monitoring System (Smoothwall)

Designated Safeguarding Lead:

• ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place;

• provides training and advice for staff;

• liaises with Local Authority / relevant body;

• liaises with school technical staff;

• receives reports of E-Safety incidents to inform future E-Safety developments;

• meets termly with Safeguarding Governor to discuss current issues,

• attends relevant meeting / committee of Governors;

• reports as and when needed to the Senior Leadership Team.

Network Manager:

• Day to day responsibility for ensuring the school's technical infrastructure is secure and is not open to misuse or malicious attack;

• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed; we currently have a password change policy for staff

• the filtering policy is applied and updated on a regular basis and includes filtering to keep children safe. This is done via Smoothwall.

• that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Designated Safeguarding Lead for investigation / action / sanction.

• that monitoring software / systems are implemented and updated as agreed in school / school policies – reviewed yearly

Teaching and Support Staff

• they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices;

• they report any suspected misuse or problems to the IT Network Manager

• E-Safety issues are embedded in all aspects of the curriculum and other activities;

• students understand and follow the E-Safety and acceptable use policies;

• they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices;

• in lessons where internet use is pre-planned, students 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.

• they are aware of the risks posed by the online activity of extremist and terrorists groups, be vigilant and alert to changes in a child's behaviour which could indicate that they may be at risk and in need of help or protection – and report this to the Designated Safeguarding Lead for further investigation, who will decide if it is appropriate to refer to the Channel program.

Students

- 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;

• should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school;

• be aware of the dangers of exposure to terrorist and extremist and other inappropriate materials and know how to report it.

Parents / Carers

Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

• digital and video images taken at school events;

• access to parents' sections of the website / on-line student / student records;

• their children's personal devices in the school (where this is allowed).

Community Users

Community Users who use school IT equipment/systems/software or access the internet within school will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems

Policy Statements

Education – students

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 curriculum should be provided as part of ICT / PHSE / other lessons and should be regularly revisited;

• key E-Safety messages should be reinforced as part of a planned programme of assemblies and form activities;

• students should be taught in all lessons to be critically aware of the materials they access online and be guided to validate the accuracy of information;

• students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;

• students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;

• 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 students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit;

• it is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be written, with clear reasons for the need and reviewed when the research is complete.

Education – parents / carers

The school will seek to provide information and awareness to parents and carers through:

• curriculum activities;

• letters, newsletters, web site;

• parents / carers' evenings / sessions;

• high profile events / campaigns e.g. Safer Internet Day;

• reference to the relevant web sites / publications e.g. www.swgfl.org.uk

www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

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

Training will be offered as follows:

• a planned programme of formal E-Safety training will be made available to staff;

• this E-Safety policy and its updates will be presented to and discussed by staff in INSET days or twilights, in morning briefings and via email.

• the Designated Safeguarding Lead will provide advice / guidance / training to individuals as required.

Training for Governors will be offered in a number of ways:

• via an e-learning course on E-Safety

• participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Managing Email

Students and staff may only use approved e-mail accounts on the school system and students must inform a member of staff immediately if they receive an offensive e-mail.

Students must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

Personal use of IT for staff and students is not permitted under this policy.

The forwarding of chain letters is not permitted.

Incoming e-mail should be monitored and attachments should not be opened unless the author is known. There is a disclaimer in place for all external email.

Managing Website Content

Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

Photographs of students will not be used without the written consent of the student's parents/carers.

The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or student's home information will not be published.

The Headteacher or the Administration and Marketing Manager will have overall editorial responsibility and ensure that all content is accurate and appropriate.

Parents/carers of new intake students and those admitted during the school year will be informed of the school procedures on image taking and publishing and their consent will be sought via the school's data pack.

Technical – infrastructure / equipment, filtering and monitoring

Reddish Vale High School will be responsible for ensuring that the infrastructure is as safe and secure as is reasonably practicable and that policies and procedures approved within this policy are implemented.

Reddish Vale High School will ensure that the staff roles identified in the above sections will be effective in carrying out their E-Safety responsibilities:

•reviews and audits of the safety and security of school technical systems will be carried out.

• physical access will be restricted to core infrastructure hardware through the use of an access control system;

• all users, staff, students and guests, will have clearly defined access rights to school technical systems and devices;

• all users will be provided with a username and secure password by the IT Department. Student credentials will be stored in a location to which staff have access. Staff are responsible for the security of their username.

• internet access is filtered for all users through our web filter. Content lists are regularly updated and internet use is logged and regularly monitored. All requests for allowing filtered content must be made via email to the IT Network Manager and with a minimum of 24 hours' notice;

• the school's technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Staff Acceptable Use of IT Policy.

• all E-Safety or technical concerns should be reported in the first instance to the IT Network Manager. Any E-Safety concerns will immediately be passed onto the Designated Safeguarding Lead. Technical concerns will be dealt with by the IT Network Manager/IT Engineer and updates provided through the helpdesk;

• the school implements and sustains an up-to-date anti-virus programme. The IT department reserve the right to confiscate any item detected as providing a threat to the integrity of the network infrastructure;

• users are not permitted to download/install executable files and/or applications on School devices. All installations must be requested through the IT department. Any unauthorised installations will be removed from devices.

• Any School device that is lost/stolen must be reported within 24 hours to the IT department. This is also a data breach and should be reported to the HT/DPO immediately.

Appendix 1

Staff & Visitor ICT Acceptable Use

1. Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and visitors will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will endeavour to ensure that staff and visitors have good access to digital technology to enhance their work, to enhance learning opportunities for students and will, in return, expect staff and visitors to agree to be responsible users.

Abuse of the internet may lead to disciplinary action being taken.

2. Acceptable Uses

As a general principle, internet access is provided to employees to support work related activities. The following list is not intended to be a definitive list, but sets out broad areas of use that the school considers acceptable uses of the internet:

- To provide communication within the school via email or the school website
- To provide communication with other schools and organizations for educational purposes
- To provide access to online systems that support teaching and learning or any other function of the school
- To distribute details regarding school meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions.

3. Unacceptable Uses

The following uses will be regarded as not acceptable, this is not a definitive list:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment.
- Use of non-educational games.
- To solicit personal information with the intent of using such information to cause emotional or physical harm.
- Entering into a commitment on behalf of the school (unless you have explicit permission to do this).
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about RVHS, your colleagues and/or our pupils on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Revealing confidential information about RVHS in a personal online posting, upload or transmission - including financial information and information relating to our pupils, staff and/or internal discussions
- Use of personal email to communicate with or about any RVHS students

- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of malicious software into the corporate network
- To disrupt the work of other users. This includes the propagation of computer viruses and use of the internet.
- Use of any Bit torrent systems
- Use for personal or private business purposes.

4. Netiquette

The following general principles should be adopted:

- Be polite. Do not be abusive in messages to others.
- Use appropriate language. Remember that you are a representative of the school and that you are using a non-private network.
- Do not disrupt the use of the internet by other users: e.g. downloading large files during lesson times and other high volume activities.

5. Email

- Whenever e-mail is sent, the sender's name, job title, e-mail address and the school's name must be included.
- Every user is responsible for all mail originating from their user ID (e-mail address).
- Every user is responsible to minimize the impact of SPAM emails. Do not click on links or open attachments unless the source is known and trusted, if you have any queries please seek the advice of the Network Manager.
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
- Attempts to send junk mail and chain letters are prohibited.
- If you receive e-mail from outside the school that you consider to be offensive or harassing, speak to your line manager (harassing internal e-mail will be dealt with under the school's guidelines).
- You should be aware that, in the event of the school being involved in legal proceedings, any relevant e-mails (including internal e-mail) may have to be disclosed, on the same basis as is the case for written documents.
- Email should be accessed via school ICT equipment only, if you wish to use a personal device to download school emails, you must ensure that your device is secured by a password at all times, that this password is not shared with any other person and that all reasonable care is taken to prevent unauthorised access to confidential information.

6. Social Networking Sites

Social media applies to blogs, microblogs like Facebook, Twitter, Bebo, LinkedIn, Videos, MySpace, social networks, discussion forums, wikis, and other personal webspace. The Governing Body at this school does not permit the use of social media on work premises unless it is strictly for the purpose of your role.
When using social media on personal devices or at home:

- Do not "speak" for the school unless you have express permission to do so, this covers all comments relating to the school
- Do not publish or comment on anything that will bring the school into disrepute
- Protect yourself from identity theft
- If you can be linked to the school, act appropriately. This includes photos and status updates
- Remember that colleagues, prospective employers, parents and children may see your online information
- School policy is that you are not allowed to be 'friends' with students until they have left us by three years, unless there are exceptional circumstances, e.g. child, sibling etc.
- Please choose your 'friends' carefully, especially in light of the point above. Ensure your settings are on private and only you and YOUR friends can see them.
- If in doubt, please seek advice in school.

7. Office 365 and One Drive

Office 365 allows access to email, online office programs and files to support teaching and learning. Professional values must be followed when using the software at all time. Below are the key points for the use Office 365 and One Drive –

- Use of the software is only permitted whilst an employee at RVHS

8. Monitoring and Logging

Activities regarding network transactions will be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current GDPR guidelines. Daily safeguarding reports are collected and emailed to the schools DSL and Safeguarding Officer for further investigation.
Such records and information are sometimes required - under law - by external agencies and authorities. The school will comply with such requests when formally submitted.

9. Wireless Network

Staff are permitted to use the school wireless network with RVHS ICT equipment for school purposes. Staff are NOT permitted to connect personal mobile phones to the school wireless network. On some occasions it may be necessary for staff to use personal laptops on the school wireless network, access will be granted at the discretion of the school Network Manager, the device will need to be checked that it is suitable for use. All use of the school's wireless network will be subject to the same monitoring and safeguarding systems.

If you are given access to the Wireless Network code for a designated school purpose, you are not permitted to share this with any other person.

10. Remote Access

Remote access to the school network is possible where this has been granted by the ICT Department.
Remote connections are considered direct connections to the school network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.
All connection attempts are logged.

11. GDPR

GDPR guidelines must be followed at all times, particularly in relation to the access, collection, storage and sharing of personal data. Only collect what is necessary and what you have a legal basis to collect, obtain consent where necessary, do not share any information unless you have permission to do so or a legal obligation to do so, and only share what is necessary. Please ensure you are familiar with the principles of GDPR.

12. Disciplinary Action

Disciplinary action may be taken against employees who contravene these guidelines, in accordance with the school's disciplinary procedures.

13. Advice

If you require any advice on the use of these guidelines, please contact the Network Manager or the Designated Safeguarding Lead.

I have read and agree to abide by the rules stated in the ICT Acceptable Use Policy. I understand the consequences if I do not.

Name: _____ **Job Title:** _____

Signed: _____ **Date:** _____

Appendix 2

Pupil Guidelines for Network Use – Acceptable Use Statement

General

Pupils are responsible for good behaviour on the school network just as they are in a classroom or a school corridor.

The school network is provided for you to do educational research to support your school work, access online educational resources and somewhere for you to save your school work. Your parents/carer's permission is required before you are allowed to use it and there is space at the bottom of this for them to sign.

Remember the motto: "Access is a privilege, not a right" and that access requires responsibility.

When you access the computer system in school and the internet, you will be given your own username and password. You are responsible for your behaviour and any Internet activity you have while on the network. You must comply with school standards and honour this agreement that you will sign.

In the interest of your safety, we may review files to ensure that you are using the system responsibly.

The following are not permitted within the school environment, this is not a definitive list:

- Sending or displaying offensive messages or pictures.
- Using obscene language.
- Harassing, insulting or attacking others (cyber bullying)
- Damaging computers, computer systems or computer networks.
- Violating copyright laws.
- Using others' passwords or accounts
- 'Hacking' into others' folders, work or files for any reason.
- Intentionally wasting limited resources, including printer ink and paper.
- Infringing copyrighting laws

Sanctions

- If you break any of the above rules and misuse your access to the internet, you may receive either a temporary or permanent ban on your internet/computer use.
- Your parents/carers will be informed.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour, including cyberbullying.
- If necessary, police or local authorities may be asked to get involved.
- If necessary, external agencies such as Social Networking or Email Member sites may be contacted and informed.

Pupils

- You must have a supervising member of staff with you at all times when using the internet.
- Do not tell anyone your password or login name, other than the persons responsible for running and maintaining the system.
- Do not upload/send personal addresses, telephone / fax numbers or photographs of anyone (*staff or pupil*) at the school through email or Social Networks.
- Do not download, use or upload any material which is copyright. Always seek permission from the owner, before using any material from the internet. If in doubt, do not use the material. This includes downloading videos and songs.
- Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children. This applies to any material of a violent dangerous or inappropriate context. If you are unsure ask your teacher

- Always respect the privacy of files of other users.
- Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Report any incident which breaches these rules to your teacher or a trusted adult in school.

I have read and agree to abide by the rules stated in the ICT Acceptable Use Policy. I understand the consequences if I do not.

Name: _____ **Form:** _____

Signed: _____ **Date:** _____

Parent/Carer _____ **Date:** _____