Reddish Vale High School

Positively changing lives through personal growth and academic excellence

E-Safety Policy

Date Reviewed: October 2025

Date Approved by Governors: February 2026

Date of next review: October 2026

RESPECT - ASPIRATION - DETERMINATION - INDEPENDENCE

Contents:

1. 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.

2. 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 that the leadership team and relevant staff are aware of and understand the systems in place, manage them effectively whilst knowing how to escalate concerns when identified.

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

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

12) 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.

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

3. The 4 key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

4. 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 Designated Safeguarding Lead 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.
- take lead responsibility for understanding the filtering and monitoring systems and process in place

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, for example, through the use of Impero.
- 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).

5. 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, for example, through the use of Impero.
- 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)
- Staff will receive annual cybersecurity training

6. 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.

7. 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.

8. 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. 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 Endpoint Protection. 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.

9. Additional support

The following websites are extremely helpful when dealing with cyberbullying and e-safety issues.

• Ceop
Child Exploitation and online Protection Centre
www.ceop.police.uk

• Bullying Online
Advice for children, parents and colleges
www.bullying.co.uk

• Virtual College
www.safeguardingchildrenea.co.uk

Kidsmart
An Internet safety site from Childnet, with low-cost leaflets for parents.
www.kidsmart.org.uk

Think U Know?
Home Office site for students and parents explaining Internet dangers and how to stay in control.
www.thinkuknow.co.uk/

Safekids
Family guide to making Internet safe, fun and productive
www.safekids.com

Maths Doctor
How To Keep Your Child Safe Online
http://www.mathsdoctor.co.uk/online/child-safety

UK Safer Internet
https://www.saferinternet.org.uk/

Appendix 1:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 2:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**