THE REACH FREE SCHOOL

Online Safety Policy

1. Monitoring and Review

This policy will be monitored by the Governing Body and reviewed every two years. However, it is recognised that this policy may need to be reviewed and revised ad hoc in response to developments in technology.

Created: August 2014
Revised: March 2022
Ratified by the Governing Body: September 2014
Date of Last Review: October 2023June 2022
Date of Next Review: June 2024

Change History	Date	Change(s) Made	Change Author	EDI[1]
V1.8	October 2023	Updates to DSL level of access and inclusion of assistant headteacher role. Modification to Reach Beyond, removal or Cyber-Know-How.	ANO/ RBO	Yes
V1.7	June 2022	Updated to recognise our working relationship with Cyber Protect and Cyber Choices programmes. Update to Online Safety Agreement regarding mobile phone use by pupils.	ASM/ SHO	Yes
V1.6	March 2022	Sections 7 and 8 updated to include references to the additional filtering and monitoring systems used.	RBO/ ANO	
V1.5	May 2021	Section 5.2 added to reflect education for parents. Section 8 updated as MDM is no longer used. Added Online Safety Agreement to the appendix of the policy	RBO/ SHO	
V1.4		Updated terminology in line with latest DfE guidance ‘e-safety’ to ‘online safety’. Inclusion of Online Safety House Assemblies.	ASM	
V1.3		Policy updated to amend the roles of the Deputy Headteachers and other minor procedural changes	RBO	
V1.2		Updated 8.2 to include web filtering at school/home	RBO	
V1.1		Reviewed the policy to ensure it meets latest DfE statutory requirements about keeping children safe when using the school network and added a bullet point about the Cyber Know How event	RBO	
V1.0		Policy created	NSI	

2. Introduction

The internet and associated technologies are an excellent tool and resource to enrich learning, however there are dangers related to their use, especially in relation to young people. Some examples of this are:

- Bullying via instant messaging or email
- Obsessive internet or gaming use
- Exposure to inappropriate material
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

As a school, it is our duty of care, alongside that of parents and other members of the community, to protect our children from these dangers and this can be achieved by many different mechanisms working together. The purpose of this online safety policy is to outline what measures the school takes to ensure that pupils can work in a safe online environment and

[1] Any changes or revisions to the policy have considered equality, diversity and inclusion.

that any online safety issues are detected and dealt with in a timely and appropriate fashion.

The Counter-Terrorism and Security Act 2015 was implemented in July 2015 and this policy sets out how the school meets its statutory requirements in respect of this, particularly around teaching pupils how to stay safe online and the web filtering the school uses. This policy has close links with the Preventing Extremism and Radicalisation Policy.

3. Aims

The Reach Free School recognises that the internet and world wide web are an essential part of life and work in the twenty-first century. However, with the use of such technology comes significant responsibility. As such, The Reach Free School will ensure:

- The internet is first and foremost a tool for learning
- Pupils are educated about safe use of the internet and world wide web
- Pupils and staff are aware of The Reach Free School's rules for the use of the internet
- The safe and acceptable use of the internet
- The online safety of all stakeholders. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

4. Audience

This document is intended for public viewing as well as that of stakeholders of the school including pupils, staff, parents, guardians and carers and the local community and is a clear outward statement on the school's online safety practices.

5. Whole school responsibilities for online safety

Within the school all members of staff and pupils are responsible for online safety, responsibilities for each group include:

5.1 Pupils

- Participate in and gain an understanding of online safety issues and the safe responses from online safety training sessions
- Comply with all acceptable use policies, which pupils must agree to when they join the school
- Report any online safety issue to a member of staff or parent, guardian or carer.
- Take responsibility for their own actions when using the internet and communications technologies.

5.2 All Staff

- Have a clear understanding of online safety issues and the required actions from online safety training sessions
- Report any online safety issues to their Line Manager, SLT or DSL as soon as the issue is detected
- Comply with all related policies

5.3 Teaching Staff

- Educate pupils on online safety through specific online safety schemes of learning and reinforce this training in the day-to-day use of ICT in the classroom.
- Ensure that technology is used safely and with purpose in the classroom.

5.4 Deputy Headteacher - Curriculum

- Works with the Headteacher to create, review and advise on online safety

- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.
- Keeps parents, guardians and carers informed of general online safety matters
- Ensures that the best technological solutions are in place to ensure online safety as well as possible, whilst still enabling pupils to use the internet effectively in their learning
- Ensures that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner, in addition to securing and preserving evidence of any online safety breach
- Deals with online safety breaches from reporting through to resolution
- Monitors the technology systems, which track pupils' internet use to detect online safety breaches
- Assists in the resolution of online safety issues with the Headteacher and other members of the Senior Leadership Team
- Maintains a log of all online safety issues

5.5 Deputy Headteacher - Inclusion

- Works with the Headteacher to create, review and advise on online safety
- Leads the development of the online safety education programme for pupils and staff
- Assists in the resolution of online safety issues with the Headteacher and other members of the Senior Leadership Team

5.6 Headteacher

- Oversees the whole IT provision at the school, ensuring that it is fit for purpose
- Works with outside agencies including the police where appropriate

5.7 Assistant Headteacher - IT

- Overseas the filtering and monitoring of school web traffic
- Ensures the DSL groups have the correct level of access to view specific online concerns
- Responds to site block and unblock requests from staff and, where applicable, pupils
- Support the pastoral teams with access to information on pupils' online footprints where required for behavioural or safeguarding purposes
- Ensure the Chromebooks issued to all pupils and staff are enrolled and managed by the school and can be monitored and tracked if required
- To ensure the filtering policies are up to date and ensure the protection and filtering in school is mirrored when pupils use their device at home
- Works with the Headteacher to ensure procurement of suitable filtering and monitoring services
- To manage the day-to-day management of the Google Admin console and regularly review the settings and application access pupils have access to
- Periodically check popular sites visited and trends to ensure filters for inappropriate sites are up to date

6. How the school ensures online safety in the classroom

6.1 Educating pupils in online safety

A role of the school is to educate pupils in the safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any online safety issues to occur.

Through Computing lessons, Reach Beyond, House Assemblies and visiting speakers from recognised providers, pupils will receive specific online safety lessons aimed at ensuring that:

- Pupils know the online safety risks that exist and how to identify when they are at risk.
- Pupils know how to mitigate against online safety risks by using safe practices whilst online.

- Pupils know when, how and to whom to report instances when their online safety may have been compromised.
- Pupils know that they are in an environment that encourages them to report online safety issues without risk of reprimand, humiliation or embarrassment.

The school will promote the Think U Know programme by the Government’s Child Exploitation and Online Protection (CEOP) centre as one of the education tools alongside the National Cyber Security Centre ‘Cyber Protect’ and ‘Cyber Choices’ programmes delivered by Herts Police. In addition to this all members of staff will have a duty to reinforce online safety practices wherever possible and will offer pupils advice and support in the classroom where minor online safety incidents have occurred.

6.2 Educating parents in online safety

The school will keep parents, guardians and carers abreast of how to support and monitor their child's online usage, and will also work alongside/involve them in any online safety concern involving their child. This can be in the form of:

- Parent educational/information events
- Sharing information via the school newsletter
- Targeted signposting for specific parents of pupils who have been involved in an online safety incident
- Up-to-date links on the school website

7. Acceptable Use Policies

All pupils and their parents, guardians and carers must adhere to the acceptable use policies before they can use the equipment provided by the school. With respect to online safety, the policy details:

- The users’ responsibilities
- Activities which are appropriate and inappropriate
- Best practice guidelines
- How the school will monitor online safety
- What information is collected

8. How online safety is monitored

- Senior leaders periodically review internet access logs to track any websites which could potentially present an online safety issue
- Senior leaders and the safeguarding team will review internet access logs and pupil communication if any content is flagged by the monitoring software
- Senior leaders will periodically review the monitoring system to track any trends and use the information to look at ways of improving the pupils’ online safety
- Teaching staff will directly monitor the pupils’ ICT and internet use in the classroom
- The monitoring and filtering software alerts the DSL group to any concerns. These concerns are followed up and details added to CPOMS, the schools’ safeguarding systems, where applicable.

9. How technology is used

The school employs a number of different technologies to help to ensure the online safety of pupils and staff:

- The school has sophisticated filtering systems provided by Hertfordshire Internet Connectivity Services, RM SafetyNet and Securly, which actively monitor pupils’ use of devices and the internet.
- The school can also restrict which activities the pupils can perform using the internet through the filtering system.

- Teaching staff will follow the behaviour policy as a deterrent for pupils who use the internet for anything other than educational purposes.

9.1 Admin Console

The school has a one-to-one device programme which ensures pupils have the tools necessary for 21st century learning. These devices are controlled and monitored by an admin console. The admin console also controls app deployment and ensures that pupils have minimal unsecured access to the device. The devices are registered to the school's domain and this cannot be removed. The school is also able to track the location of a device, supporting missing or lost devices.

9.2 Web Filtering and Monitoring

Web filtering has changed in recent years, now it is more about allowing access to valuable learning resources, as opposed to blocking all content. The school uses web filtering to block inappropriate content and websites which are irrelevant to the pupils' programme of study and are considered time wasting.

The school receives filtered web access from Hertfordshire Internet Connectivity Services and RM SafetyNet. This automatically categorises inappropriate content, blocking unsuitable material. However, the system allows the flexibility to access and block sites as required. This role is undertaken by the Senior Leadership Team. In addition to this, devices have an additional filtering and monitoring system provided by Securly. Whenever a device is connected to the internet, including outside school, the content will be monitored and filtered. Parents, guardians and carers should continue to ensure appropriate parental controls are set on their home internet provider.

10. How the school will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a pupil or staff member infringes the Online Safety Policy, the final decision on the level of consequence will be at the discretion of the Headteacher.

10.1 Pupils

10.1.1 Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone/tablet (or other new technologies) during the school day e.g. to send texts to friends
- Use of unauthorised instant messaging/social networking sites.

Possible consequences: referral to SLT, removal of device until end of day, contact with parent, guardian or carer, removal of internet access rights for a period.

10.1.2 Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Accidentally accessing offensive material and not notifying a member of staff

Possible consequences: referral to SLT, removal of device until the end of week, contact with parent, guardian or carer, removal of internet access rights for an extended period, exclusion.

10.1.2 Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the internet
- Transmission of commercial or advertising material
- Any other action that could be deemed to cause offence or hurt to another person

Possible consequences: referral to SLT or Headteacher, contact with parents, guardian or carer, removal of equipment, removal of internet, exclusion, referral to police.

10.1.3 Category D infringements

- Continued sending of emails or instant messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 1988, as amended
- Bringing the school name into disrepute.

Possible consequences: Referral to SLT or Headteacher, exclusion, removal of equipment, referral to police.

11.1 Staff

11.1.1 Category A infringements (Misconduct)

- Excessive use of the internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first-level data security, e.g. wrongful use of passwords
- Breaching copyright or licence e.g. installing unlicensed software on a network.

Possible consequences: Referred to line manager, SLT or Headteacher, warning given.

11.1.2 Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software
- Any deliberate attempt to breach data protection or computer security rules
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 1988, as amended
- Bringing the school into disrepute.

Possible consequences: Referred to Headteacher and Governing Body to follow disciplinary procedures, police.

12. Child Pornography

In the case of child pornography being found, the member of staff will be immediately suspended and the school disciplinary procedures implemented.

12.1 Other safeguarding actions

- Remove the equipment to a secure place to ensure that there is no further access to it
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school
- Identify the precise details of the material
- Where appropriate, involve external agencies as part of these investigations.

13. How will staff and pupils be informed of these procedures?

- Procedures are included within the school's Online Safety Policy available via the staff handbook
- Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'. Pupils will be required to sign an age appropriate online safety form
- The school's online safety policy will be made available to parents, guardians and carers who are required to sign an acceptance form when their child receives their own device.

14. Working with parents, guardians and carers

Clearly many pupils will also have access to ICT and the internet at home, often without some of the safeguards that are present within the school environment. Therefore parents, guardians and carers must be extra vigilant about their child's online safety at home.

15. Links with Other Policies

Preventing and Tackling Bullying Policy
Behaviour Policy
Mobile Phone and Device Policy
Child Protection Policy
Preventing Extremism and Radicalisation Policy
Online Safety Agreement

THE REACH FREE SCHOOL

Online Safety Agreement

The Reach Free School actively encourages the use of electronic devices as a tool for learning and to enhance the overall learning experience. Utilising a variety of devices at The Reach Free School gives pupils the access to learn anywhere, anytime - at school and at home. This one-to-one, personalised learning also narrows the digital divide between pupils and promotes responsible use of today's ever-changing technologies.

The Reach Free School reserves the right to search and confiscate a pupil's device to ensure compliance with this Online Safety Agreement. Pupils in breach of this agreement may be subject to but not limited to; disciplinary action, overnight confiscation, removal of content or referral to external agencies. In the event of any disciplinary action, completion of all classwork remains the responsibility of the pupil. The Reach Free School is not responsible for the financial loss of any personal files that are deleted.

This agreement also relates to a pupil's own personal device.

1. I will only use the school's Information Technology (IT) equipment for school purposes.
2. I will not download or install software on the school's IT equipment.
3. I will only log on to the school's network, other school systems and resources using my own school username and password.
4. I will not reveal my passwords to anyone other than a parent, guardian, carer or member of staff. I will not use my personal email address or other personal accounts on the school's IT equipment.
5. I will make sure that all my electronic communications are responsible and sensible.
6. I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents, guardians and carers and the police if necessary. I know it is essential that I build a good online reputation.
7. I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately, to a member of staff if I am in school or parent, guardian or carer if I am not in school.
8. I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image.
9. I will immediately report any request for personal information, to a member of staff if I am in school or parent, guardian or carer if I am not in school.
10. I should never post photographs, videos or live streams without the permission of all parties involved.
11. I will not upload any images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying.
12. I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.
13. I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
14. I will respect the privacy and ownership of others' work online and will adhere to copyright at all times.
15. I will not attempt to bypass the internet filtering system in school.
16. I will not assume that new technologies can be brought into school and will check with staff before bringing in any device.

…..continued overleaf

17. I will not lie about my age in order to sign up for age-inappropriate games, apps or social networks.
18. I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents, guardians or carers before arranging to meet someone I only know on the internet.
19. I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined and my parents, guardians or carers may be contacted. If I break the law the police may be informed.
20. I will not use my mobile phone when in school
21. I may be required to take part in the Social Media Educational Programme (SMEP)

Pupil Agreement

Pupil Name:..

Pupil’s’ Form:..

I have discussed this agreement with my parents, guardians or carers and understand the commitment I have made and my responsibilities.

Pupil’s Signature:..

Date:..

Parents, Guardians and Carers Agreement

Parent(s), guardian(s) or carer(s) name(s):..

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with my child. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute.

Rather than posting negative material online, any parent, guardian or carer distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school impact on the reputation of the whole school community. Parents, guardians and carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and their families.

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s), Guardian(s) or Carer(s) signature(s):..

Date:..

This document will be kept on file at school.