THE REACH FREE SCHOOL

E-Safety Policy

1. 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 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 e-safety policy is to outline what measures the school takes to ensure that pupils can work in an e-safe environment and that any e-safety issues are detected and dealt with in a timely and appropriate fashion.

The Counter-Terrorism and Security Act was implemented in July 2015 and this policy sets out how the school meets it 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.

2. 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 e-safety of all stakeholders. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

3. Audience

This document is intended for public consumption 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 e-safety practices.

4. Whole school responsibilities for e-safety

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

4.1 Pupils

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.
- Compliance with all acceptable use policies, which pupils must agree to when they join the

school.
- Reporting any e-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.

4.2 All Staff
- Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.
- Report any e-safety issues to their Line Manager as soon as the issue is detected.
- Compliance with all related policies

4.3 Teaching Staff
- Educating pupils on e-safety through specific e-safety schemes of learning and re-enforcing this training in the day-to-day use of ICT in the classroom.

4.4 Deputy Headteacher - Curriculum
- Works with the Headteacher to create, review and advise on e-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 e-safety matters
- Ensures that the best technological solutions are in place to ensure e-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 securing and preserving evidence of any e-safety breach
- Deals with e-safety breaches from reporting through to resolution
- Monitors the technology systems, which track pupils' internet use to detect e-safety breaches
- Assists in the resolution of e-safety issues with the Headteacher and other members of the Senior Leadership Team
- Maintains a log of all e-safety issues
- Plans and hosts the annual Cyber-Know-How event for parents, guardians and carers

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

4.6 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. How the school ensures e-safety in the classroom

5.1 Educating pupils in e-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 e-safety issues to occur.

Through Technology lessons and REACH Time pupils will receive specific e-safety lessons aimed at ensuring that:

- Pupils know the e-safety risks that exist and how to identify when they are at risk.
- Pupils know how to mitigate against e-safety risks by using e-safe practices whilst online.
- Pupils know when, how and to whom to report instances when their e-safety may have been compromised.
- Pupils know that they are in an environment that encourages them to report e- 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. In addition to this all members of staff will have a duty to reinforce e-safety practices wherever possible and will offer pupils advice and support in the classroom where minor e-safety incidents have occurred.

6. 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 e-safety the policy details:

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

7. How e-safety is monitored

- Senior leaders periodically review internet access logs to track any websites which could potentially present an e-safety issue
- Senior leaders will periodically review the monitoring system to track any trends and use the information to look at ways of improving the pupils' e-safety
- Teaching staff will directly monitor the pupils' ICT and internet use in the classroom.

8. How technology is used

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

- The school has a sophisticated system, which actively monitors the pupils' use of the internet. This system alerts a senior member of staff to any potential e-safety issues.
- The school will 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.

8.1 Mobile Device Management (MDM)
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 a robust MDM using a profile system. The profiles are registered to the device allowing for monitoring to take place. The MDM also controls app deployment and ensures that pupils have minimal unsecured access to the device, notifying the relevant person when profiles are removed.

8.2 Web Filtering
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 unfiltered web access from Hertfordshire Internet Connectivity Services and filters the content onsite using a third party web filtering system. 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.

When a school device, ie iPad or Chromebook is connected to the internet outside the school system, the content will be unfiltered. Parents, guardians and carers must ensure appropriate parental controls are set on their home internet provider as set out in the iPad Home Use

Agreement.

9. 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 E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher.

9.1 Pupils

9.1.1 Category A infringements

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

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

9.1.2 Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone/ tablet (or other new technologies) after being warned
- Accidentally accessing offensive material and not notifying a member of staff

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

9.1.2 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

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

9.1.3 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 sanctions – Referral to SLT or Headteacher, exclusion, removal of equipment, referral to police.

10.1 Staff

10.1.1 Category A infringements (Misconduct)

- Excessive use of 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 network.

Possible sanctions - Referred to line manager, SLT or Headteacher, warning given.

10.1.2 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 sanctions – Referred to Headteacher and Governing Body to follow disciplinary procedures, police.

11. Child Pornography

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

11.1 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.

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

- Procedures are included within the school's E-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 e-safety form
- The school's e-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.

13. 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 e-safety at home. In order to ensure e-safety at home it may be necessary for the school to:

- Run training sessions and workshops on e-safety as part of the 'Parents as Pupils' sessions
- Publish e-safety information and direct parents, guardians and carers to external e-safety advisories via the school website.

14. 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.

15. Links with Other Policies

Preventing Bullying Policy

Created: August 2014
Revised: March 2018
Ratified by the Governing Body: September 2014
Date of Last Review: March 2018
Date of Next Review: Spring 2020

Change History	Change(s) Made	Change Author
V1.0	Policy created	NSI
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
V1.2	Updated 8.2 to include web filtering at school/ home	RBO
V1.3	Policy updated to amend the roles of the Deputy Headteachers and other minor procedural changes	RBO