Acceptable Use Policy (AUP)

Rivington Foundation Primary School

This Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.
This AUP is for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. (From Feb 2017)

The agreement is a partnership between parents/carers, pupils and the school to ensure that users kept safe when using technology.

Users of technology will be made aware of any children who, for whatever reason, are not allowed to access technology , this list must be kept in school and made available to the staff.

AUP will:

- Be regularly reviewed and updated.

- Be regularly communicated to all users, particularly when changes are made to the eSafety Policy/AUP.

- Outline acceptable and unacceptable behaviour when using technologies.

Unacceptable behaviour:

- Cyberbullying – targeting of individual by group or individual person

- Inappropriate use of email, communication technologies and Social Network sites and any outline content. Any illegal activity – which **will** be reported to the relevant authorities, without exception.

Examples of illegal offences are:

- Accessing child sexual abuse images

- Accessing non-photographic child sexual abuse images

- Accessing criminally obscene adult content

Incitement to racial hatred **Dealing with incidents**

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the Head Teacher who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF).

Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Always report potential illegal content to the Internet Watch Foundation. They are licensed to investigate – schools are not!

Acceptable behaviour

- Uphold the School Safeguarding and Child Protection Policies
- Always use passwords
- Respect filtering of content
- Report any failings in technical safeguards immediately.
- Always make DSL Deputy DSL, aware of network activity and online communications connected to classroom activity.
- Have high regard for importance of eSafety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

Approved by Governors as a policy separate to e-safety Feb 2017