RUSH COMMON ACADEMY TRUST
A COMPANY LIMITED BY GUARANTEE
COMPANY NUMBER 7931886

E-SAFETY POLICY FOR RUSH COMMON SCHOOL

Introduction

In this policy as in all documents of Rush Common Academy Trust ("RCAT") any reference to Governors of Rush Common School or Trustees of RCAT is a reference to the Board of Directors of RCAT and any reference to the Headteacher of Rush Common School is a reference to the Chief Executive Officer of RCAT.

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Rush Common School's E-Safety Policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Prevent Duty (2015), Curriculum, Data Protection and Security.

E-Safety depends upon effective practice at a number of levels:

- Responsible Information and Communication Technology (ICT) use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure including the effective management of content filtering.
- National Education Network standards and specifications.

The School has appointed an E-Safety Co-ordinator.

Our E-Safety Policy has been agreed by the E-Safety Focus Group. It has been and approved by the Leadership Team and Directors of RCAT.

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents/carers will be informed that pupils will be provided with supervised internet access.
- Parents/carers will be asked to sign and return a consent form for pupil access. Failure to do so will mean that the pupil will not be allowed to access the internet in school for any purpose but the pupil will still be able to use the computer for non-internet based activities.

World Wide Web

- Any use of unsuitable sites by children should be reported as an incident to the E-Safety Co-ordinator and subsequently included in the Headteacher's Report to RCAT.
- The School will ensure that the use of internet derived materials by pupils and staff complies with Copyright Law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

School Web Site

- The School website will be used to provide up-to-date information regarding the School.
- The Leadership Team will take overall editorial responsibility and ensure that content is accurate and appropriate.

Digital Storage

- The School uses RM Unify as its main means of secure on-line storage within the school.
- Membership is restricted to members of the School community (pupils, staff, and the Board of Directors).
- Usernames and passwords are provided for all members.
- Content is regularly monitored by the E-Safety Co-ordinator.

Email

- All members of staff are required to use the approved e-mail accounts only for official school business.
- Pupils may only use approved e-mail accounts within school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- 'InTouch' is used by the School as the main means of communicating electronically with parents/carers.

Sharing Photographs

- Photographs of activities taken within school or during school trips are only taken on school cameras or iPads.
- Pupils' full names will not be used anywhere on the school website.
  Pupils' work can only be published with the permission of parents/carers.
- Photographs of special activities are stored securely on Picasa Web Albums. Parents may be provided with a link to a particular album, but these are not visible to the general public.

Mobile Phones

- Mobile phones will not be used for personal use during lessons or formal school time by members of the teaching staff.
- Pupils may only bring mobile phones to school if they have prior permission from the Headteacher (see Mobile Phone guidance).

Filtering

The School will work in partnership with relevant agencies and bodies and the internet Service Provider (ISP) to ensure filtering systems are as effective as possible.
Filtering is in place to ensure that learners are unable to access terrorist and extremist material online through School servers.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Publishing Pupils' Images.
- On admission to the School, parents/carers will have the opportunity to give their consent to the publishing of photographs within the Learning Platform.
- Specific permission will be requested before publishing photographs on any public space.

Information System Security

- School ICT systems' capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed and agreed with the leadership team and professional bodies, as necessary.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Assessing Risks

- The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the School nor RCAT can accept liability for the material accessed, or any consequences of internet access.

- A log will be kept of any incidents of internet misuse within the School.
- A regular audit of ICT use will be carried out to establish if the E-Safety policy is adequate and that the implementation of the E-Safety Policy is appropriate.

Handling E-Safety Complaints

- Complaints concerning internet misuse will be dealt with by the E-Safety Co-ordinator.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents/carers will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for internet access will be posted on all networked equipment.
- Pupils will be informed that internet use will be monitored.

Staff

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff are aware of the online risks posed by online activity of extremist and terrorist groups, as with other online risks of harm.

Preventing Radicalisation

The Counter Terrorism Act (2015) and Keeping Children Safe in Education document (July 2015) places responsibility on schools and other agencies to ensure that they have due regard to the need to prevent people from being drawn into terrorism.

School has a duty to identify and report on any issues where someone may be identified as being drawn into terrorism or extremist views (violent or non-violent). We work with social care, the police, health services and other services (including Oxfordshire Safeguarding Children's Board) to promote the welfare of children and protect them from harm.

We have clear procedures in place for protecting children at risk of radicalisation. There is no single way of identifying an individual who is likely to be susceptible to a terrorist ideology. Staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Even very young children might show signs of radicalisation.

The Designated safeguarding Lead can make a referral about any adult (to Social and Healthcare Team) or child, who school think may be vulnerable to being drawn into terrorism, via the safeguarding team (MASH) or by calling the police (999) or on 101 for non-urgent concerns.

Parents/Carers

- Parents/carers' attention will be drawn to the School E-Safety Policy on the school website.
- Parents/carers will be made aware of regular E-Safety lessons within the School.

Review of this Policy

The Board of the Directors of RCAT, through its Pupil Support and Welfare Committee, review this policy every year. It may however, review this policy earlier than this if the government introduces new regulations, or if it receives recommendations on how this policy might be improved.

Approved by the Pupil Support and Welfare Committee of the Board of Directors of RCAT on 1st December 2015

Signed: C Wilmshurst (Chair of Board of Directors)

Signed: L Youngman (Headteacher)

Date for Review: December 2018