ONLINE SAFETY POLICY FOR RUSH COMMON SCHOOL

Introduction

Online 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 Online Safety Policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Prevent Duty (2015), Curriculum, Data Protection and GDPR.

Online 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 online 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 Online Safety Co-ordinator.

Our Online Safety Policy has been and approved by the Leadership Team and Governors of LAB.

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 Online Safety Co-ordinator and subsequently included in the Headteacher's Report to LAB.

- 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 Headteacher and Deputy Headteacher will take overall responsibility for ensuring that content is accurate and appropriate.

Digital Storage

- The School uses Google Drive 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 Governors).
- Usernames and passwords are provided for all members.
- Staff are expected to alert the Online Safety Co-ordinator of any inappropriate use of Google Drive.

Email

- All members of staff are required to use the approved e-mail accounts only for official school business.
- Staff are required to encrypt/password protect all emails which contain sensitive, personal information
- Pupils may only use approved e-mail accounts within school.
- Pupils must immediately tell a teacher if they receive an 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. ParentMail is used by the School as the main means of communicating electronically with parents/carers.

Sharing Photographs

- Photographs of activities taken by staff/school representatives within school or during school trips are only taken on school phone or iPads.
- Pupils' full names will not be used anywhere on the school website unless permission has been granted.
- Pupils' work can only be published with the permission of parents/carers.
- Photographs of special activities are stored securely on Google Drive.
- Parents are reminded they are not to share photos on social media.
- Permission forms for photo use of pupils are sent out annually to parents.

Mobile Phones

- Mobile phones will not be used for personal use during lessons or formal school time by members of the teaching staff.
- Mobile phones must not be used to take any images of children during school time.

- Pupils may only bring mobile phones to school if they have prior permission from the Headteacher (see Mobile Phone guidance).

Filtering

- The school uses filtering software to prevent unauthorised access to illegal websites.
- The Online Safety Co-ordinator and IT support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.
- Filtering also ensures that learners are unable to access terrorist and extremist material online.

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.

Information System Security

- School IT systems' capacity and security will be reviewed regularly.
- Virus protection is installed and updated regularly.
- Security strategies are 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 2018, following data protection principles which state that information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

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 LAB can accept liability for the material accessed, or any consequences of internet access.
- CPOMs will be used to record any incidents of internet misuse within the School.
- A regular audit of IT use will be carried out to establish if the Online Safety policy is adequate and that the implementation of the Online Safety Policy is appropriate.

Handling Online Safety Complaints

- Complaints concerning internet misuse will be dealt with by the Online Safety Coordinator.
- 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 PCSOs to establish procedures for handling potentially illegal issues.

Social Media

- The school makes use of social media as a means of communication, ensuring that parents give permission.
- No pupils, parents or school staff names will be used in any post.
- Staff do not engage in online discussion on personal matters relating to members of the school community.

Communication of Policy

Pupils

- Pupils receive regular Online Safety lessons throughout the school year through both the Computing and PSHE curriculum.
- Pupils will be informed that internet use will be monitored.

Staff

- All staff are made aware that the School Online Safety Policy and its importance explained.
- Staff are made 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 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 nonviolent). 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 need 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 Online Safety Policy on the school website.
- Parents/carers will be made aware of regular Online Safety lessons within the School.

Review of this Policy

The Board of the Governors of LAB, through its Pupil Support and Welfare Committee, review this policy every three years. 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 Board of Governors of LAB December 2022

Signed: *Debbie Lymn* **(Chair of Board of Governors)**

Signed: *Kristen Fawcett* **(Headteacher)**

Date for Review: December 2025