Embracing Empathy | Achieving Excellence | Unlocking Opportunities

Online Safety Policy

See also, Safeguarding Policy, Staff Handbook & Positive Workplace Policy

Date	
Signed	

Introduction

Redbourn Park School has a duty to provide students with quality internet access as part of their learning experience. Students will be taught what internet use is acceptable and what is not and given clear objectives for its use. All staff involved with teaching and learning will prepare students to benefit safely from the opportunities presented and ensure that they have a growing understanding of how to manage the risks involved in online activity by:

- ❖ Discussing, reminding or raising relevant online safety messages with students routinely, wherever suitable opportunities arise.
- ❖ Reminding students, colleagues and parents/carers about their responsibilities, which have been agreed through the User Agreement (Appendix 1) that all students and parents/carers have signed.
- ❖ Staff will guide students to online activities that will support the learning outcomes planned for the students' age and maturity. Access levels will also be reviewed to reflect curriculum requirements.
- ❖ Teaching students as a planned element of personal, social, health, economic and citizenship education about online safety, cyber-bullying, misuse of technology, the law in this area and how to correctly use modern technology for positive reasons.

MANAGING AND SAFEGUARDING COMPUTER SYSTEMS

It is our leadership team's role to ensure that the security of the school's systems and its users are reviewed regularly. It is also the role of staff to monitor students and report any concerns, as they would with any child protection concern. The schools current systems include:

- ❖ Virus protection is installed and current on all laptops used for school activity.
- ❖ Access by wireless devices is proactively managed (students cannot access the school's wireless network from their personal devices).
- ❖ Portable media may not be used without specific permission.
- ❖ Mobile Device Management is deployed across devices on and off site which allows leaders to monitor and secure devices remotely via an internet connection.
- ❖ Unapproved software is not allowed on any school machines.
- ❖ Any administrator or master passwords for school IT systems are kept secure and available to at least two members of staff, e.g. head teacher and the designated safeguarding lead.
- ❖ No-one except the IT consultants, Head Teacher or designated safeguarding lead is allowed to approve a download or authorise an install software onto the network.
- ❖ New users can only be created and approved by a member of the leadership team.
- ❖ Any laptops or school technology taken off the school site must be used in accordance with this and all other relevant school policies and any damage or loss is at the expense of the staff member.
- ❖ Access to the internet has two layers of filtering. Firstly, user level access is in place, giving different permissions and restricted access to software and websites to staff and students. Secondly, the wifi network also has a layer of filtering and monitoring leaders can update, adapt and restrict either types of content or specific websites. Access to the network and our systems is also protected through both systems.

INTERNET ACCESS

The school maintains a simple internet connection that requires a password to access. This password is not shared with students, but visitors are able to use it to connect to the internet if required. The router can be accessed to restrict usage and content available to users within the school. Leaders/ICT teachers can also restrict or approve websites as required. Again, students are never left unsupervised when they are on the

internet on the computers. This software is also vital in securing protection/inability to cheat when students are sitting formal functional skills exams online too.

EMAIL

Email is regarded as an essential means of communication and all employees are provided with an email account. Communication by email from teaching staff and administration staff to parents/carers and to external organisations should be related to school matters only. Email messages related to school matters should reflect a suitable tone and content, ensuring that the good name of the schools is maintained. The same procedures are expected of all other employees who send emails to external organisations and colleagues. Use of the school's email system is monitored and checked and staff should not use personal email accounts during school hours or for professional purposes. Staff are not permitted to use school email accounts to communicate with students directly at any time. See our data protection policy for further information on use of email and storing documents on Google Drive.

PUBLISHING MATERIAL ONLINE

www.Redbournpark.co.uk

Redbourn Park School maintains editorial responsibility for website content to ensure that the content is accurate and the quality of presentation is maintained. The schools maintain the integrity of their website by ensuring that responsibility for uploading material is always moderated and that passwords are protected. The identities of students are protected at all times.

Photographs of identifiable individual students are not published on the website unless parents/carers have provided written permission for the school to use students' photographs. Photographs never have names attached

Students publishing online (blogs and websites)

In some instances, it may be appropriate for students to use websites or blogs to complete, or celebrate, their work. As always, the identities of students must be protected at all times. Photographs of identifiable individual students are not published unless parents/carers have provided written permission for the school to use students' photographs. Photographs must never have full names attached (first name or initials only) and no personal information that could be used to identify them should be disclosed. Parents/carers must have given specific permission via the user agreement forms to allow students to create websites or blogs.

Other online communication platforms

Staff and students are encouraged to adopt similar safe and responsible behaviour in their personal use of blogs, wikis, social networking sites and other online publishing inside and outside of school hours. Material published by students and staff in a social context which is considered to bring the school's reputation into disrepute or considered harmful to, or harassment of, another child or member of the organisation will be considered a breach of conduct and behaviour and treated accordingly, as per behaviour, equality, anti bullying and/or staff conduct policies/procedures.

USING IMAGES, VIDEO AND SOUND

Redbourn Park School recognises that many aspects of the curriculum can be enhanced by the use of multimedia and that there are now a wide and growing range of devices on which this can be accomplished. Students are encouraged and taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of students wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

All parents/carers are asked to sign an agreement about taking and publishing photographs and video of their students when offered a school or activity placement and this list is checked whenever an activity is being photographed or filmed. For their own protection, staff or other visitors to our premises are discouraged from using a personal device (mobile phone, digital camera or digital video recorder) to take photographs of students or visitors.

MOBILE PHONES

Students are discouraged from bringing mobile phones into school but if they do, they typically hand them to the office for safekeeping until the end of the school day. Some students may keep their mobile School staff are not to use mobile phones during the school day, with the exception of calling the school or the emergency services if an emergency situation arises whilst off-site (eg. school trips). Staff are not encouraged or expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a child or parent/carer. Unauthorised or covert use of a mobile phone or other electronic device, to record voice, pictures or video is strictly prohibited.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyber-bullying', will be considered a disciplinary matter for students and staff alike. The same is the case for other inappropriate use of mobile technology, such as 'sexting'. Students are taught about misuse of technology as a matter of course through the school's personal, social, health, economic and citizenship education programme. See our 'what we do' policy for curriculum information.

NEW TECHNOLOGY

Redbourn Park School will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an online safety point of view. We will regularly review this policy to reflect any new technology that we use, or to reflect the use of new technology by students.

Employees, visitors or students using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

DATA

The school recognises their obligation to safeguard staff and students' personal data including that which is stored and transmitted electronically.

We ensure:

❖ Students are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties
❖ Staff are aware of their obligation to keep sensitive data secure when working on computers outside of school
❖ When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
❖ There is full back up and recovery procedures in place for school data (all child and staff data is kept securely in the 'cloud' online).

- Where sensitive, staff or child data is shared with other people who have a right to see the information, for example professionals in social care teams, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies.
- Please also refer to our Data Protection policy.

ONLINE SAFETY INCIDENTS

All incidents, including online safety incidents, are recorded on our incident sheets. Any incidents where students do not follow the User Agreement will be dealt with following the school's 'how we do it' (behaviour policy) and procedures. In situations where a member of staff is made aware of a serious online safety incident, concerning students, visitors or staff, they will inform a senior leader who will respond in the most appropriate manner. Instances of cyber-bullying will be taken very seriously and will be dealt with using the school's preventing bullying procedures and the organisation's disciplinary procedures. The organisation recognises that staff as well as students may be victims and will take appropriate action in either situation.

If an action breaches school policy, appropriate sanctions will be applied. The schools will decide if parents/carers need to be informed if there is a risk that child data has been lost. Redbourn Park School reserves the right to monitor their premises equipment and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

GOVERNANCE

The Education (Independent School Standards) Regulations apply a duty to proprietors of independent schools to ensure that arrangements are made to safeguard and promote the welfare of children. The body of governance at Redbourn Park School consists of a governing body. The governing bodies ensure that they comply with their duties under legislation and fulfil their duty to remedy any weaknesses that are identified.

In relation to online safety, duties and responsibilities include:

- The proprietor and governors will ensure that appropriate filters and monitoring systems are in place, across all of the sites to ensure that students are safeguarded from potentially harmful and inappropriate material.
- The proprietor and governing body will ensure that children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum.

APPENDIX 1

STUDENT COMPUTER & INTERNET USER AGREEMENT

THIS MUST BE SIGNED BY BOTH STUDENT AND PARENT/CARER BEFORE INTERNET ACCESS IS ALLOWED

Use of ICT considers the use of the school's technology and internet. As part of a society that where technology is used regularly, students must have the opportunity to learn appropriate and positive ways of using technology. At Redbourn Park School, students are expected to be responsible for their own behaviour on computers and the internet, just as they are anywhere else in school. In order for us to allow internet use, student and parents must read and agree to the Use of ICT Agreement.

Use of ICT Agreement:

- ❖ I will only access the system through the proper log-in and will keep my password secret from others
- ❖ I will not access other people's files
- ❖ I will only use the computers for school work and homework
- ❖ I will not bring CDs or other storage devices from outside school unless I have been given permission by a teacher
- ❖ I will not use rude language in my work
- ❖ I will ask permission from a member of staff before using the internet
- ❖ I will not download any files from the internet
- ❖ I will not try to access social media sites or instant messaging services
- ❖ I will not email people unless teachers approve it
- ❖ I will never give out my personal details online
- ❖ If I see anything rude, or anything that worries or upsets me, I will tell a teacher immediately
- ❖ I understand the school may check my computer files and internet usage
- ❖ I will only use approved websites and all communications will be supervised and appropriate
- ❖ I know that if I break these rules, I may lose access to the computers and internet in school

If parents have any concerns about their child and their use of ICT in or out of school, or would like to request support in ensuring their home is secure and has the appropriate parental controls in place, please contact a member of staff and we will make every effort to support you.

Name _____ Date_____

Sign_____

Last Review	August 2024	Next Review	August 2025	Owner	Head Teacher

Published on	
By	
Chair of Gov Sig/date	
Head Teacher sig/date	

Staff read and acknowledged:

Name	Sig/Date