**Pear Tree Primary School incorporating PiPs Before and After School Club**



 

E-Safety Policy

|  |  |
| --- | --- |
| Date agreed | September 2020 |
| Date for Review | September 2024 |
| Headteacher | Boo Edleston |
| Chair of Governors | Simon Holden |
| Signed on behalf of the Governors’ Board by:Name:  | Signature:Date:  |
| Signed on behalf of the school by:Boo EdlestonHeadteacher | Signature:Date: |
| Reviewed by: Richard Pickup | Date: September 2022 |

 1.  **INTRODUCTION**

The E-Safety Policy also relates to other policies including those for IT, anti-bullying and safeguarding.

Our E-Safety Policy has been written by the school, building on the Brine Leas High School E-Safety policy.

## 2. TEACHING AND LEARNING

###  2.1 Why Internet Use is Important

* The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
* Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
* Currently access to the internet and online resources/learning is an essential requirement in order to carry on with pupil education. The risk of classroom or school closures means the continuity and connection with the school that is provided by internet access are more important than ever.

###  2.2 Internet use will enhance learning

* The school Internet access will be designed expressly for pupil and staff use and will include filtering appropriate to the age of pupils.
* Pupils and families will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
* Home learning platforms provide extra levels of monitoring and review of pupils learning.

###  2.3 Pupils will be taught how to evaluate Internet content

* The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
* Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## 3. MANAGING INTERNET ACCESS

###  3.1 Information system security

* School IT systems and security will be reviewed regularly.
* Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.

###  3.2 Email

* Pupils may only use approved e-mail accounts on the school system.
* Pupils must immediately tell a teacher if they receive offensive e-mail or any other social media communication when in school.
* 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 an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
* Where email addresses are required for home learning, then they will not be configured to work as actual email addresses, but just as logins for any future system that requires them (e.g. Microsoft Teams/Google Classrooms etc..)

###  3.3 Published content and the school web site

* The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils’ personal information will not be published in line with our privacy notice.
* The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

###  3.4 Publishing pupil’s images and work

* Photographs that include pupils will be selected carefully and will adhere to the permissions given by parents. Pupils’ full names will not be used anywhere on the Web site, particularly in association with photographs.
* Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
* Pupil’s work can only be published with the permission of parents.
* Work sent over any home learning platform is not published, but instead is only available to the pupil, classroom teacher or any relevant staff.
* In cases where work is shared amongst the class electronically (either via a home learning platform or video platform such as Zoom) then this will be known in advance.

###  3.5 Social networking and personal publishing

* Pupils will be advised never to give out personal details of any kind which may identify them or their location.
* Pupils and parents may be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
* Staff are advised that they should consider the consequences and possible repercussions of any information that they make available online, for example on a social networking site. Particular care should be taken in the posting of photographs, videos and information related to the school, school life, staff and pupils as detailed in the staff code of conduct document.
* 3.5.1. School based Social Media such as Microsoft Teams
* If a school based social media platform is to be used (such as Microsoft Teams) then staff will make pupils aware that whatever is posted on there is available to everybody including staff.
* Staff can setup separate groups for themselves and other members of staff, where sharing of resources or general communication is required, again consider that anything posted in those channels is visible to all members of the channel.

### 3.6 Managing filtering

* The school will work with the LA, DCFS and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator who should be known to all members of the school community.
* Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

###  3.6.1 Home Learning Considerations

* There is no possibility of managing filtering when a pupil uses computers at home, either a school provided iPad or Laptop or their own/family’s device. It is therefore recommended that children do not access the internet without supervision.

### 3.7 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.

* Mobile phones are not allowed for pupil use on the school premises.
* Staff will not use personal equipment or non-school personal electronic accounts when contacting families.

### 3.8 Protecting personal data

• Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the GDPR regulations 2018.

### 3.9 Data Security

• Files stored by the school will be backed up locally and remotely so that in the event of a system failure, ransomware attempt or general loss of data, the files are stored in the cloud and can be recovered by our support team.

## 4. POLICY DECISIONS

### 4.1 Authorising Internet access

* All staff must read and sign the ‘Staff Code of Conduct and Social Media policy’ before using any school IT resource.
* All students and their parents must sign the permissions in their school diaries relating to permissions and all classes are reminded of safety rules of internet and social media usage.

### 4.2 Assessing risks

* The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the internet provider can accept liability for the material accessed, or any consequences of Internet access.
* The school will regularly audit IT provision to establish if the e-safety policy is adequate and that its implementation is effective.
* Links to 3rd party content, such as webpages and worksheets that are provided electronically will be checked before being shared. However due to the nature of the internet, links and sites can change over time along with the content that was originally provided. It is recommended that any linked content is downloaded as soon as possible to avoid the content changing.

### 4.3 Handling e-safety complaints

* Complaints of Internet misuse will be dealt with by a senior member of staff.
* 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 will be informed of the complaints procedure.
* Discussions will be held with the Police Officer to establish procedures for handling potentially illegal issues.

## 5. COMMUNICATIONS POLICY

### 5.1 Introducing the e-safety policy to pupils

• E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.

 Pupils will be informed that network and Internet use will be monitored.

 **5.2 Staff and the e-Safety policy**

* All staff will be given the School e-Safety Policy and its importance explained.
* Staff should read this policy in conjunction with the Acceptable Use Policies.
* Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

### 5.3 Enlisting parents’ support

Parents’ attention will be drawn to the School e-Safety Policy on the school Website.

* Where possible the school will provide additional advice on e-Safety and general internet safety awareness, either via newsletters or advice, or as working with the parents in groups to raise awareness.

## 6. Remote Learning / Online-Distributed Homework

### 6.1 Online work

• Where work has been distributed via an online platform such as Microsoft Teams, it is the responsibility of the child/parent to access the work and complete and return as necessary. Information on how to do this will be given by staff at the school

• Interaction with the messaging system such as Chat in Microsoft Teams is monitored and any inappropriate usage will be dealt with by staff at the school as a serious matter.

• When live online video sessions are necessary, there must always be at least 2 members of staff present, and we recommend that a parent/carer be in the room or nearby at the children’s side of the session.

• Direct messaging between children has been disabled and the only method of communication using the platform is fully public for all to see.

• Only staff can create meetings and online sessions and let people in to them via the use of a waiting room/lobby system.

• Once a session has ended staff will terminate the session which will remove all other participants from the meeting/video session.

• Logging into another person’s account without their permission, impersonating somebody else, or accessing other people’s files are all considered inappropriate behaviour and will be dealt with as a serious matter by the school.

**A**