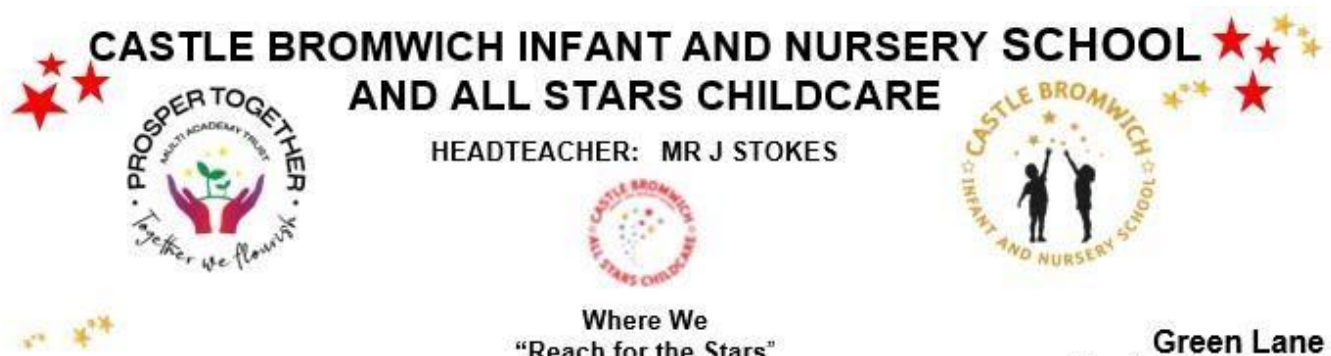




E-Safety Policy

Date: March 2024 – March 2027



Castle Bromwich Infant & Nursery School E-safety Policy 2024

Writing and Reviewing the E-safety Policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for Computing, behaviour, PSHE, dignity at work and child protection.

The school has appointed an e-Safety subject lead: Carley Johnstone

Our e-Safety Policy has been written by the school, building on the Solihull e-Safety Policy and government guidance. It has been agreed by senior leadership and approved by Governors.

Teaching and Learning- Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.

Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet, in order to locate, retrieve and evaluate information.
- Pupils are shown how to publish and present information to a wider audience.

-

-

Pupils will be taught how to evaluate Internet content

- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils will be taught the importance of not believing everything they read on the Internet.
- Pupils will be taught how to report unpleasant Internet content e.g. telling and showing a trusted adult, minimising the page or switching the monitor off.

Managing Internet Access

Information system security

- We use the experts employed by the MAT and the Local Authority to support us in this area and act fully on their recommendations.
- Virus protection is updated regularly.
- We use the Unity collaborative security strategies to protect our Network.

E-mail

- Staff and pupils may only use school e-mail accounts on the school system to send emails relating to school.
- Pupils must immediately tell a teacher if they receive offensive e-mails.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Pupils are taught how to use emails safely via the PurpleMash website.
- Pupils will only use school email to email people they know via the PurpleMash website.
- The forwarding of chain letters is not permitted.

Published content and the school website/social media

- Staff or pupil personal contact information will not be published. The contact details given online will be the school's office account.
- The Head Teacher takes overall editorial responsibility and to ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, extranet or social media.
- Work will only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.

-
-
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others. They should be advised not to publish specific and detailed private thoughts.

Managing filtering

- The school works with Solihull Local Authority to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the eSafety Coordinators and this is then reported to the Local Authority.

Managing emerging technologies

- Emerging technologies are examined for educational benefit before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff should not use their mobile telephone for taking photographs of children. Staff should use school devices when taking photographs in school or on trips. • Appropriate use of the Extranet (Learning Platform) is detailed in the School's Acceptable Use Policies.
- Children should not bring any devices into school. (smart phones, smart watches, iPads, tablets)

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018. All Data held by 3rd parties conforms to the GDPR.

-
-
- Memory sticks and laptops to be encrypted according to Local Authority policy.

Policy Decisions

Authorising Internet access

- All staff must read and sign the Staff Acceptable Use Policy before using any school ICT resource.
The school maintains a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a child's AUP consent form.
- Any person working in school will be asked to sign the Staff Acceptable Use Policy before being allowed to access the internet from the school site.
All Staff must sign the e-Safety Monitoring Compliance document, confirming they are aware all keystrokes and internet use is monitored.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to fully guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Solihull Local Authority can accept liability for any material accessed, or any consequences of Internet access. However, the school filtering system and the staff's awareness of e-safety allows us to take as many precautions as possible
- The school audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety co-ordinators.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents are informed of the complaints procedure (see school's complaints policy) Pupils and parents are informed of consequences for pupils misusing the Internet.

Use of the Internet beyond the school day

- The school liaises with community organisations (before/after school care) and parents/carers to establish a common approach to e-safety.

-

-

Communications Policy

Introducing the e-safety policy to pupils

- E-Safety rules and objectives are posted in all rooms where computers are used and discussed with pupils regularly.

-
-
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- A programme of training in e-Safety will be undertaken by staff as appropriate.
- E-Safety training is embedded across all areas of the curriculum.

Staff and the e-Safety policy

- All staff are given the School e-Safety Policy and its importance is explained.
- Staff are informed that network and Internet traffic can be monitored and traced to the individual user.
- The school uses kids safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site and Extranet.

The school will direct parents to the Extranet where there are e-safety resources for parents/carers.

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

