Jesse Gray Primary Online Safety Policy

Head Teacher Signature:	
Date Adopted:	**May 2023**
Review Date:	**May 2024**

Contents:

Writing and reviewing the online safety policy

The online safety policy is an important part of day-to-day routines and safeguarding throughout school, also it relates to other policies including those for Computing, anti-bullying and for child protection. The school's computing leader will also act as online safety coordinator, alongside the PSHE coordinator.

Our online safety policy has been written by the school, building on the LA, the Rushcliffe schools alliance and Government guidance.

It has been agreed by SLT and approved by governors. The Online Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why safe 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 children with quality Internet access as part of their learning experience. Internet use is also a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The Internet access within school is designed expressly for pupil use and includes filtering appropriate to the age of pupils without over-blocking content. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. They will be taught how to deal with a range of issues online, including accessing content. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. 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.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated on an ongoing basis
- Advice on security strategies will be monitored and clarification sought as necessary.
- Broadband connection will be via an approved supplier and will include suitable filtering abilities.

E-mail

- Pupils may only use approved e-mail accounts on the school system and email usage will be supervised and monitored by a staff member.
- Pupils must immediately tell a teacher if they receive offensive or worrying e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils will not send emails to anybody outside the school.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The use of the school twitter handles and account will be monitored by the computing coordinator and members of management but is each teacher's responsibility to ensure the content published on their pages follows the guidelines set out by school. It should not give personal details or information. See the Twitter policy.
- Class webpages are updated by class teachers, who have been briefed on the appropriate content for publishing.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and pupils will remain anonymous, only using their initials.
- Pupils' full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or Twitter page and this will be done at the point the child enters the school.
- Pupil's work can only be published with the permission of the pupil and parents.
- Parents are briefed at the start of any performance or public event on the appropriate sharing of any media taken.

Social networking and personal publishing

- The school will block/filter access to social networking sites, excluding Twitter for teacher use.
- Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- All staff need to be aware that any contact with pupils via personal email or social networking sites, texting and other forms of electronic communication is contrary to Nottinghamshire County Council advice and current safeguarding children directives and is therefore not permitted. This applies in all settings. This is to protect both pupils and staff.

Managing filtering

- The school will work with the LA, DfE 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 Computing Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- All pupils are prohibited from bringing mobile phones to school except in pre agreed circumstances/procedures.
- Mobile phones belonging to staff will not be used during lessons or formal school time [See also Mobile phone policy]. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- From May 2018, any data processing will comply with the data protection law under the General Data Protection Regulation (GDPR).

<u>Policy Decisions</u>

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using school ICT resources.
- For Key Stage 1, access to the Internet will be by adult demonstration, or directly supervised access to specific, approved online materials.
- In Key Stage 2, children will be expected to learn how to use the internet independently, but direct supervision should be maintained at all times.

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 NCC can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online 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 head teacher; if it is the head teacher a complaint is being made about, then it should be made to the Chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be made aware of the complaints procedure. If any illegal internet use is suspected, then the police will be notified.

Communicating the Policy

Introducing the online safety policy to pupils

- Pupils will be informed that network and internet use will be monitored.
- Online safety will be taught in a variety of ways across the curriculum.
- Pupils'/parents'/staff members' views concerning online safety will be sought and used to inform future developments in online safety education.
- Online safety will be introduced to pupils alongside addressing anti-bullying in PSHE, to ensure the risks and strategies for dealing with anti-bullying run through all forms of communication. They will be explicitly taught cyber-bulling as a form of bullying and ways to prevent and tackle it.

Staff and the online safety policy

- All staff will be given the School online safety policy and its importance explained.
- Training on online safety issues will also be provided.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website.
- Regular online safety training for parents can be arranged.
- Parent's views will also be sought and used to inform future developments in online safety education.

APPENDIX

Jesse Gray Primary - Staff Guide to Internet Use.

These guidelines need to be followed by all staff:

- Only use websites that are appropriate.
- Staff are expected to adopt a professional approach to their use of the internet
- Do not use personal social media accounts, chatrooms, Instant Messaging Services in school.
- Please check memory sticks for viruses before using them on school equipment.
- Memory sticks cannot be used unless they are password protected and encrypted.
- Do not give out your passwords for email, Google drive or similar.
- It is forbidden under current safeguarding directives to have any personal contact with children via electronic means, unless via Seesaw (please see NCC Contact Policy).

  This includes not allowing pupils' access to your pages on any social networking sites you may be a member of, giving children your mobile number, or letting them access a private e-mail account.
  Contact for professional purposes only is acceptable via a dedicated school email Google account.

  If you are wondering if something is a good idea, then ask or don't do it at all.

Jesse Gray Staff, Governor and Visitor - Acceptable Use Policy/ICT Code of Conduct

Computing and the related technologies such as email, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of technology. All staff are expected to sign this policy and adhere at all times to its contents.

- I appreciate that computing includes a wide range of systems and devices including mobile phones, PDAs, digital cameras, email, social networking and may include personal devices when used for school business.
- I understand that it is a criminal offence to use a school technology system for a purpose not permitted by its owner.
- I will comply with the computing system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activities carried out under my user name.
- I will only use the school email, internet, intranet, Learning platform or any related technologies for professional purposes.
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the head teacher or governing body.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without permission.
- I will ensure that my online activity both in school and outside school will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's online safety policy and help pupils to be safe.
- I will report any incidents of concern regarding children's safety to the computing coordinator and the head teacher.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature

I agree to follow the code of conduct and support the safe use of ICT throughout the school.

Full Name: _____

Job Title: _____

Signature_____ Date_____