Internet and e-safety Policy

Rationale

College Park Infant School and Lyndhurst Junior School are committed to developing our pupils' Computing capabilities and supporting their families. It is vital that we also aid our staff in improving their own knowledge and skills for teaching, learning and their own professional development. We are aware that we live in an ever-changing technological world and wish to embrace the current and future technologies. However, this area is open to misuse and school policies and practices are in place to safeguard and protect all users.

Why is internet use 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 national curriculum and a necessary tool for staff and pupils.

Purposes

Our schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

This policy also takes into account the National Curriculum Computing programmes of study and the Early Years Foundation Stage Curriculum requirements. It complies with our funding agreement and articles of association.

Processes

<u>Educating pupils about online safety</u>

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite visitors and speakers to talk to pupils about this.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be available to parents along with a shorter summary leaflet, which may be more accessible.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School, Executive Headteacher and/or any other DSL at the schools.

Concerns or queries about this policy can be raised with any member of staff or the Executive Headteacher.

Managing Internet Access

Internet use will enhance learning

- The school Internet access is provided by Portsmouth City Council and includes filtering appropriate to the age of pupils. An additional filtering set is available in school administration networks only and enables staff access to additional resources.
- Pupils 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.

Pupils will be taught how to evaluate Internet content

- We aim to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Information system security

- School ICT systems capacity and security are reviewed regularly.
- Virus protection is installed and updated regularly.
- Security strategies are discussed with our technical support providers.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher, and staff tell the Head of School, if they receive 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.
- Staff to pupil/parent email communication must only take place via a school email address and will be monitored.
- 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.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the school website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head of School or nominee will take overall editorial responsibility and endeavour to ensure that content is accurate and up to date.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and used appropriately.
- Pupils' full names will not be used anywhere on the website.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Social networking and personal publishing

- Portsmouth City Council will normally block/filter access to social networking sites unless short-term access is required for a specific educational project.
- 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.
- Pupils/parents must not place personal photos/videos taken at school on any social network space without school permission.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Managing filtering

The school will work in partnership with our technical support providers and Portsmouth City Council to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported IT Services Help Desk by email helpdesk@portsmouthcc.gov.uk

Cyber-bullying

Cyber-bullying

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the schools' Anti-bullying policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will help our pupils to understand what it is and what to do if they become aware of it happening to themselves or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
The school also has an information leaflet on the Internet and e-safety so that parents are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the schools' Anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the schools' Complaints policy.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to uphold the schools' policies and procedures regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Older pupils in KS2 may bring mobile phones to school especially if they walk to and from school unaccompanied, but these must be handed into the school office before school starts and collected at the end of the school day. No other electronic devices will be allowed on school premises.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Head of School. Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the Behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training as part of safeguarding training, as well as relevant updates as required (for example through emails, online or face to face training and staff CPD).

The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policies.

Monitoring
The Heads of School log behaviour and safeguarding issues related to online safety.
This policy will be reviewed every two years by the Heads of School and then the Governors' Resources Committee.

Links with other policies
This online safety policy is linked to our:

- Child protection and safeguarding policies
- Behaviour policies
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints policy and procedures

Review
When: Bi- Annually
By whom: Resources Committee of the Local Governing Board
Agreed: November 2018