The Park College
Learning for life

ONLINE SAFETY POLICY

The purpose of this policy is to:

- Outline the key principles expected of all members of the college community at The Park College regarding the use of ICT
- safeguard and protect the students and staff of The Park College assist college staff working with students to work safely and responsibly with the internet and other communication technologies
- set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other college policies
- ensure that all members of the college community know unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken

Scope of the policy

This policy applies to all members of college community - staff, students, volunteers, parents and carers, visitors, community users - who have access to and are users of college's ICT systems.

Communication of the policy

The policy will be:

- Displayed on the college website
- Included as part of the induction pack for new staff
- Saved in the policies folder in the staff shared area
- Shared through the Acceptable Use policy agreed with all staff.

Responding to complaints

- The college will take all reasonable precautions to ensure online safety. However, it is not possible to guarantee that unsuitable material will never appear on a college computer or mobile device. Neither the college nor the Local Authority can accept liability for material accessed, or any consequences of internet access.
- Staff and students are informed of the possible sanctions related to misuse of technology and these are outlined in the Behaviour Policy.
- Our online safety coordinator is the Designated Lead for Safeguarding and is the first point of contact for any complaint. Any complaint about staff misuse will be referred to the Principal.
- Complaints that relate to online bullying will be dealt with in line with our Safeguarding Policies.

Student online safety curriculum

The college has a clear, progressive online safety education programme primarily as part of the Computing curriculum / PSHE curriculum but referenced in all areas of college life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The college will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities when on-line.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.

The college will ensure that:

- Staff understand the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information.
- Regular training is available to staff on online safety issues and the college's online safety education programme.
- Information and guidance on the Safeguarding policy and the college's Acceptable Use Policy is provided to all new staff and governors.

Parent engagement

The college recognises the important role parents and carers have in ensuring students and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the college in this area we will provide:

- Regular, up to date information in newsletters and on the website, particularly in response to emerging trends.
- Face to face sessions in college.
- Opportunities to share in their student's online safety learning
- Support and advice on online safety for their students outside of college.
- Signposting to further resources and websites.

Conduct

All staff are responsible for using the college ICT systems in line with the Acceptable Use Agreements they have signed. They should understand the consequences of misuse or accessing inappropriate materials.

All members of the college community should know that this policy also covers their online activity outside of college if it relates to their membership of the college.

All staff will:

- read, understand and help promote the college's Online Safety policies and guidance
- read, understand, sign and adhere to the college staff Acceptable Use Agreement
- be aware of Online Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current college policies regarding these devices
- report any suspected misuse or problem to the Online Safety coordinator
- maintain an awareness of current Online Safety issues and guidance
- model safe, responsible and professional behaviours in their own use of technology

Incident Management

All members of the college community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively. The college actively seeks advice and support from external agencies in handling online safety issues. Parents and carers will be informed of any online safety incidents relating to their own child, unless doing so may put the child at risk. All parents and carers will receive more general online safety advice in response to incidents, without revealing any sensitive or personal information about students.

Managing the ICT infrastructure

The college is responsible for ensuring that the college infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their online safety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the college meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the college's technical systems.
- All users will have clearly defined access rights to the technical systems and college owned devices.
- All users will be provided with a username and secure password. Users will be responsible for the security of their username and password.
- The administrator passwords for the college ICT system, used by the Network Manager (or another person) is also available to the Principal and kept in a secure place.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The college allows different filtering levels for different groups of users – staff / students.
- The college regularly monitors and records the activity of users on the college technical systems and users are made aware of this in the Acceptable Use Agreement.
- There is a reporting system in place for users to report any technical incident or security breach.
- Security measures are in place protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the college systems and data. These are tested regularly. The college infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the college site unless safely encrypted or otherwise secured.

Data

The college has a Data Protection and Handling Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; the responsibilities of the Senior Information Risk Officer (SIRO); and the storage and access of data.

Staff Use of Mobile Technologies

Personal mobile phones and mobile devices brought in to college are the responsibility of the device owner. The college accepts no responsibility for the loss, theft or damage of personal mobile phones or mobile devices.

Staff are not permitted to use their own mobile phones or devices for contacting students, young people or their families within or outside of the setting in a professional capacity.

Mobile phones and other devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or other personal devices will not be used during teaching periods.

Staff should not use their own devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

Personal mobile phones can be used for college duties – e.g. in case of emergency during off-site activities.

Private numbers can be withheld by dialling 141 first.

Student Use

Student mobile phones must be kept in lockers. They can be accessed at break times.

Authorised staff can search student's electronic devices if they have good reason to think that the device has been or could be used to cause harm. Any search will be carried out in by two members of the management team.

Digital images and video

We seek permission from parents and carers for the use of digital photographs or video involving their child when their child joins the college.

We do not identify pupils in online photographic materials or include the full names of students in the credits of any published college produced video.

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission.

Students are taught about the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or college.

Social networking

- Staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students.

College staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or college staff;
- They do not engage in online discussion on personal matters relating to members of the college community
- Personal opinions should not be attributed to the college or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Review and Monitoring

Online safety is integral to other college policies including the Safeguarding Policy, Anti-bullying Policy and Behaviour Policy. The college's online safety coordinator is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and online safety issues in the college. This policy has been developed and approved by the Senior Leadership Team and Governors. Staff will be informed of any updates or amendments to it.