The Park College
Learning for life

The Park College Online Safety Policy

Aims

Our college aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and directors
- Deliver an effective training programme around online safety, which empowers us to protect and educate the whole college community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- **The 4 key categories of risk**
- Our approach to online safety is based on addressing the following categories of risk:
- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Roles and Responsibilities

The board of directors: have overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The board will receive regular reports from the principal and designated safeguarding leads (DSL) on the implementation of the college policy.

The board will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on the Acceptable Use Policy
- Ensure that online safety is a running and interrelated theme within the college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, training about safeguarding, including online safety, is adapted to meet the needs of all students because of the importance of recognising that a 'one size fits all' approach is not appropriate for all students in all situations, and a more personalised or contextualised approach may often be more suitable.

The Principal: is responsible for ensuring

- all staff understand this policy

- the policy is implemented consistently throughout the college
- all online safety incidents are logged and dealt with appropriately in line with this policy
- all incidents of cyber-bullying are dealt with appropriately in line with the college behaviour policy

The designated safeguarding lead and deputy designated safeguarding leads

Details of the DSLs are set out in the college safeguarding policy.

The DSL and DDSL take lead responsibility for online safety in college, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the college
- Working with all staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the college safeguarding policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the college behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in college to the Principal or governing board

This list is not intended to be exhaustive.

The ICT contractor: is responsible for

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material
- Ensuring that the college's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting full security checks and monitoring the college's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

All staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the college's ICT systems and the internet, and ensuring that students follow the college's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Families

- Families are expected to:
- Notify the Principal of any concerns or queries regarding this policy
- Support students in learning to use ICT safely in line with the college policy
- Families can seek further guidance on online safety on our website and from the following organisations:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the college's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on the Acceptable Use Policy.

Online safety and the college training programme

Students will be taught about online safety as part of the curriculum. Our Online Safety curriculum is personalised to meet the needs of individual students. It develops knowledge and understanding across the following key areas:

- Using technology safely and respectfully, responsibly and keeping personal information private
- Identifying where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Recognising acceptable and unacceptable behaviour
- Identifying a range of ways to report concerns about content and contact
- Students develop understanding:
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to people they may encounter (in all contexts, including online) whom they do not know
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of students (including those created by students) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other areas of the college training programme where relevant.

Our teaching about safeguarding, including online safety, is adapted to meet the individual developmental needs of each student.

Working with families

The college raises families' awareness of online safety through our newsletters, website and face to face events. Bespoke support is provided for groups and individual families. This policy is available to all families and online safety is included in annual reviews.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the principal.

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

Cyber-bullying

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 college behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The college will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

The college also shares information on cyber-bullying with families so that they are aware of the signs, how to report it and how they can support anyone affected.

In relation to a specific incident of cyber-bullying, the college will follow the processes set out in the college behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the college 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.

Examining electronic devices

College staff will work with families and students if they have concerns about content on students' electronic devices. The principal / DSL will consider if 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 college rules
- If inappropriate material is found on a device the principal / DSL will follow current guidance on

- Direct the student to delete that material, or
- Retain it as evidence (of a criminal offence or a breach of college discipline), and/or
- Report it to the police*
- If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with students and young people.

College staff will not search student devices. Concerns will be shared with the DSL / Principal.

Acceptable use of the internet in college

All staff, volunteers and board members are expected to sign an agreement regarding the acceptable use of the college's ICT systems and the internet. Visitors will be expected to read and agree to the college's terms on acceptable use if relevant.

Use of the college'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 students, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Students using mobile devices in college

Students bringing mobile phones to college must leave them in their locker. Students can access their own devices during breaks and designated times in the college day.

Staff using work devices outside college

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the college's terms of Acceptable Use Policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Principal.

How the college will respond to issues of misuse

Where a student misuses the college's ICT systems or internet, we will follow the procedures set out in our behaviour and safeguarding policies.

The action taken will depend on the individual circumstances and nature of the specific incident, and will be proportionate.

Where a staff member misuses the college'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 college 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 at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that students are at risk of online abuse
- Students can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don’t want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs 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, and at least annually.

Board members 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 policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed every year by the Principal. At every review, the policy will be shared with the Board. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with other policies

- This online safety policy is linked to our:
- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in college?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the college’s acceptable use agreement for staff, volunteers, trustees and visitors?	
Are you familiar with the college’s acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the college’s ICT systems?	
Are you familiar with the college’s approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	