Online Safety and Social Media Policy

Date of creation	July 2015
Date of last update	February 2022
Author	Chalene Scott & Costas Calcanis
Responsible Manager	Costas Calcanis
Approved by	ELT
Date of Approval	15th March 2022

Policy Statement

Barnet and Southgate College is committed to the responsibility that it has for the Safeguarding of all learners and the protection of children and vulnerable adults.

Barnet and Southgate College is also committed to providing high quality education and training and to ensuring that our students achieve to the very best of their ability. The College recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning.

The College aims, at all times, to create and maintain a safe environment for all students, staff, volunteers and visitors. This includes creating a safe 'on-line' environment for all and monitoring the acceptable use of the internet and social media related to the College. We believe this can be achieved through a combination of security measures, training and guidance plus implementation of associated policies.

Introduction

This policy sets out the principles that Barnet and Southgate College students, staff, volunteers, governors and visitors are expected to follow when using the internet and internet–based social networking media on the College premises and remotely. Any user of College IT systems and personal devices when on site, must adhere to the IT Acceptable Use Policy. The Online Safety and Social Media policy applies to all use of the internet and electronic communication devices such as e-mail, mobile phones, games consoles, social networking site and any other systems that use the internet for connection and provision of information.

Policy Aims

This Policy aims to:

- Safeguard all students, staff, volunteers, governors and visitors from risks online by ensuring College IT-based systems are strong and reliable and meet all legal requirements
- Set out codes of conduct expected of all members of the College community (student positive behaviour policy and staff code of conduct) with respect to the use of IT technologies, so as to ensure user behaviour is safe and appropriate
- Provide opportunities to educate all students, staff, volunteers and governors aboutonline safety including awareness that is unacceptable, unlawful or unsafe behaviourmay, where appropriate, result in disciplinary or legal action.
- Have procedures in place to appropriately manage online abuse, illegal activity and incidents which threaten online safety
- Support students, staff, volunteers, governors and visitors in understanding their responsibility to record and report concerns about unsafe internet usage

Definition of Online Safety

The term 'online safety' is defined for the purposes of this document as the process of limiting the risks to the College community when using Internet, Digital, Mobile Technologies (IDMTs) and Social Media platforms through a combined approach of policies and procedures, infrastructures, and education, including training, underpinned by standards andinspection.

When talking about online safety, risks can be summarised under the following headings:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, 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. If you feel your students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Incidents and response

Incidents could include (but are not limited to); illegal activity such as; gambling, bullying, peer-on-peer abuse, threats of violence/harm, hate crime, radicalisation and extremism, grooming, pornography and so forth.

Observations and concerns raised in regards to online safety incidents (i.e. accessing material which may pose potential harm) should be reported to the Safeguarding team following the College's Safeguarding procedures. This includes, but is not limited to concerns about:

- Grooming (including radicalisation and child sexual exploitation)
- Bullying and harassment
- Sharing explicit personal photos/videos
- Violence and weapons
- Peer on Peer abuse

Reports via the College's IT filter systems or breach of Acceptable Use systems will be dealtwith by either the IT services or the Safeguarding Team in the first instance.

The safeguarding team are tasked with providing appropriate support to students who have been exposed to harm or have been harmed online; whereas IT services are tasked with contacting the appropriate member of staff to sanction or offer support. This includes but is not limited to:

- Propagating viruses, worms, Trojan horses etc.
- Corrupting or destroying other users' data
- Deliberate unauthorised access

Reports of online safety incidents are acted upon in a timely manner to prevent, as far as reasonably possible, any harm or further harm occurring.

Action following the report of an incident might include further investigation, support for the student and affected students, disciplinary action, sanctions, referrals to external agencies (e.g. social services, the police, Channel, CEOP etc.), review of internal procedures and safeguards.

The responsibility for online safety is for the whole College community who should stay alertand respond to any potential or actual online concerns as described above. Everyone will be expected to take reasonable action to ensure their safety online and that of students.

Education and Training

Staff, volunteers, governors and students are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively. This is done by using a range of opportunities and methods to embed online safety and thedelivery of explicit sessions which include:

- Student inductions and tutorial programme which includes developing critical thinking skills; the risks of downloading, posting and sharing images; the risks ofposting personal information; and how to keep personal information safe.
- Staff Safeguarding induction and on-going training to comply with relevant legislation
- Student Positive Behaviour Policy
- Staff Code of Conduct
- Targeted safeguarding awareness sessions with tutor groups and individual students
- Reading and acknowledging the Acceptable Use Policy by all staff and students

Behaviour

- Appropriate behaviour and consequences of breaching the Online safety policy is set out in the IT Acceptable Use Policy, Guidance for Online tutoring, teaching and support, Staff code of Conduct and Student Positive Behaviour Policy which all users oftechnology should adhere to. This includes but not limited to:
  - Use of email, mobile phones, social networking sites, games consoles, chat rooms,video conferencing and web cameras, etc.
  - Any abuse of IT systems and any issues of bullying or harassment (cyber bullying)are dealt with seriously, in line with staff and student disciplinary procedures.
  - Any conduct considered illegal or potentially harmful
  - Violating the privacy of others or disrupting their work
  - Accessing potentially harmful sites, images or links

Social Media

The College encourages students and staff to use social media to enhance their learning experience. However, anybody who associates with Barnet and Southgate College is expected to behave in accordance with the College's values and policies and, in doing this,to maintain the College reputation. The College reserves the right to restrict access to emerging social media sites or content if required

- If a staff member wishes to set up a social media platform for their area of activity they should consult the Marketing and Communications department for advice on;branding, tone and so forth, to enable the College to keep track of its approved social media platforms.
- If a student wishes to set up a social media platform for College activity they should approach their tutor who will, in turn, contact the Marketing department.
- When using social media for College purposes staff and students must be mindful ofthe integrity, purpose and intentions of individuals, organisations and groups that are 'befriended' on accounts.
- When using social media staff and students must be made aware that their personalprofiles may be visible to a wider audience, and they should review their personal permissions on the social media accounts they use. For this reason, it is important that staff and students consent to joining these platforms by actively signing up rather than being added by site admins.
- All those using a person blog, or any other social media platform should be aware of confidentiality in their discussions around the College Community.
- If a member of staff or student post on a blog or any other social media platform and it is clear you work for or attend the College there should be a visible disclaimer such as; "these are my personal views and not those of Barnet and Southgate College".
- Individuals must not engage in activities on the Internet which might bring Barnet and Southgate College into disrepute.
- Individuals must not use the Internet in any way to attack or abuse anyone (students,colleagues, or tutors etc) for example, revenge porn, online bullying, sharing nude images, indecent images, sexting etc.
- Individuals must not post derogatory or offensive comments on the Internet
- Individuals must not write defamatory/libellous reviews about the College, students, or staff on social platforms

Use of images and video

The use of images or photographs is encouraged to enrich teaching and learning, providing there is no breach of copyright or other rights of another person. For example, there may bean expectation that photographs taken at College do not appear publicly therefore explicit permission should be sought to do this.

Staff and students should NOT post photos and information that they have been asked not to. They should remove information about a colleague or peer if asked to do so.

Personal information

Processing of personal information is done in compliance with the Data Protection Act 2018.

Security

- College networks are safe and secure, with appropriate and up-to-date security measures and software in place.
- The College has robust reporting mechanisms for any breaches of online security.

Links to Other Policies

This policy should be read alongside other College policies which includes but is not limited to; *Safeguarding and Protection of Children Policy; Equality and Diversity Policy, IT Acceptable Use, Anti-Bullying Policy, Student Positive Behaviour Policy, Staff Code of Conduct, Education and Training Foundation Professional Standards for Teachers and Trainers*

Review

This policy will be regularly monitored and reviewed in accordance with:

- Changes in legislation and statutory guidance on the safeguarding of young people and vulnerable adults.
- Governor and Safeguarding and Wellbeing Committee updates
- Key trends identified through the College's compliments, complaints and concerns process and safeguarding case reviews conducted
- Changes within the College which may impact on the processes and procedures for safeguarding young people and vulnerable adults.
- The College's annual Self-Assessment Review process to continually develop and improve practices and procedures across the organisation.

Useful Links and resources for Staff, Parents and Students

- Child Exploitation Online Protection Centre
- Internet Watch Foundation
- NSPCC Keeping Children Safe Online
- Child Net - information and guidance on a range of key online safety topics
- UK Safer Internet Centre

- Internet Matters Online Safety Advice for Teens
- Action for Children Advice for Parents to help children stay safe
- Sharing nudes and Semi-nudes Advice for education settings working with young people
- Sexting Advice for Professionals
- ACT Action Counters Terrorism Report suspicious activity related to terrorism