Online Safety and Social Media Policy

Date of creation	July 2015
Date of last update	July 2017
Next update due	July 2018
Author	Toni Beck
Responsible Manager	Toni Beck
Approved by	ELG
Date of Approval	12th August 2017
Date of Equality Impact Assessment	Equality Impact Assessment - All Documents

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 learners 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 learners, 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 learners, staff, volunteers, governors and visitors are expected to follow when using the internet and internet–based social networking media both on the College premises and remotely. Any user of College IT systems 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 learners, 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 with respect to the use of IT technologies, so as to ensure user behaviour is safe and appropriate

- Provide opportunities to educate all learners, staff, volunteers and governors about online safety including awareness that unacceptable, unlawful or unsafe behaviour may, 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 learners, 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 and inspection.

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

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to potentially harmful material, such as that inciting violence, terrorism, hate or intolerance
- Exposure to illegal material
- Illegal downloading of copyrighted materials e.g. music and films

Contact

- Grooming using communication technologies, potentially leading to abuse, radicalisation and other crime
- Bullying and harassment via websites, mobile phones or other forms of communication device

Commerce

- Exposure of children (under 18) to inappropriate commercial advertising
- Exposure and access to online gambling services
- Commercial and financial scams

Incidents and response

Incidents could include (but are not limited to); illegal activity such as; gambling, bullying, abuse, hate crime, radicalisation and extremism, grooming, pornography and so forth.

Observations and concerns from staff members in regards to online safety incidents (i.e. a learner 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

Reports via the College's IT filter systems or breach of Acceptable Use systems will be dealt with by IT services in the first instance. IT services are tasked with contacting the appropriate member of staff to sanction or support the learner involved. 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 learner and affected learners, disciplinary action, sanctions, referrals to external agencies (e.g. social services, the police, Channel etc.), review of internal procedures and safeguards.

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

Education and Training

Staff, volunteers, governors and learners 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 the delivery of explicit sessions which include:

- Learner inductions and tutorial programme which includes: developing critical thinking skills; the risks of downloading, posting and sharing images; the risks of posting personal information; and how to keep personal information safe.
- Staff Safeguarding induction and on-going training to comply with relevant legislation
- Learner Code of Conduct
- Staff Code of Conduct and 'Working with Learners : A Guide for All Staff'
- Targeted safeguarding sessions with specific groups and individual learners
- Reading and acknowledging the Acceptable Use Policy by all staff and learners

Behaviour

Appropriate behaviour is set out in the IT Acceptable Use Policy which all users of technology 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 learners 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.

- 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 learner wishes to set up a Social Media platform for College activity they should approach their tutor who will, in turn, contact the Marketing and Communications department.
- When using Social Media for College purposes staff and learners must be mindful of the 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 personal profiles 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 learner post on a blog 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 students, colleagues, teachers or tutors.
- Individuals must not post derogatory or offensive comments on the Internet
- Individuals must not write defamatory/libellous reviews about the College, learners 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 be an expectation that photographs taken at College do not appear publicly therefore explicit permission should be sought to do this.

Staff and learners 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 1998.

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 Policy including the Protection of Children and Vulnerable Adults, Equality and Diversity Policy, IT Acceptable Use, Anti-Bullying Policy, Disciplinary, Learner Code of Conduct, Staff Code of Conduct, Working with Learner a Guide for All Staff.*