S38 Student E-Safety and Acceptable Use Policy

Full Governing Body **November 2017**
Next Review: **Autumn 2019**
Responsible: **Vice Principal: Pastoral Care and Safeguarding**

1. Introduction

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

2. E-Safety Statement

The Bushey Academy works with staff, students and parents/carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential e-safety risks.

The Designated Lead for E-Safety is the Vice Principal: Pastoral Care and Safeguarding, a member of the academy's Senior Leadership Team.

The academy monitors and reviews its systems and procedures on e-safety on a regular basis, linking it with other relevant policies such as Safeguarding, Pupil Behaviour and Anti-Bullying policies. Action will be taken immediately where a breach occurs and will be in compliance with the above policies.

Staff are supported in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole curriculum.

The academy ensures that students are aware of the potential e-safety risks associated with the use of ICT and mobile technologies, that they feel able and safe to report incidents and abide by the academy's policies.

E-safety is embedded into school culture and this is supported through a comprehensive PSHCE programme, assemblies and curriculum provision. The aim is to develop students' understanding of the importance of adopting good e-safety practice when using digital technologies, as well as developing their understanding of the importance of reporting abuse, misuse, or access to inappropriate materials. They should learn how to report such instances and recognise their responsibility to do so.

Additionally, the above provision will include education around Child Sexual Exploitation (CSE), radicalisation and extremism, cyber bullying and Peer on Peer abuse. The provision will also include key messages on self-esteem and positive relationships in order to develop students' awareness and resilience when using digital technologies.

The academy also provides opportunities for parents/carers to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour both in the academy and at home.

3. This Acceptable Use Policy is intended to ensure that:

- students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The academy will work to ensure that all students have good access to digital technologies to enhance their learning and will, in return, expect students to agree to be responsible users.

The academy reserves the right to monitor all activities of users who utilise the academy's IT systems and equipment.

The Academy is committed to the statutory guidance for schools and colleges on the duty in the ***Counter Terrorism & Security Act 2015*** to have due regard to the need to prevent children, young people & adults from being drawn into terrorism. Keeping children safe from risks posed by terrorist exploitation of social media will be approached in the same way as safeguarding children from any other on-line or off-line abuse. The academy will ensure suitable online safety internet filtering, firewalls and automatic internet alerts, are in place to ensure that children are safe from terrorist and extremist material when accessing the internet through the academy network and follow the Prevent Duty safe practice guide.

4. Acceptable Use Agreement – Students

Students will use academy ICT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users.

Students:

- will keep usernames and passwords safe and secure. Students will only use the password allocated to them by the academy to gain access to the IT systems. Passwords will be kept securely and will not be shared. Students will not attempt to gain unauthorised access to the system through other methods
- will not disclose or share personal information about themselves or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, etc)
- will immediately report to staff any unpleasant or inappropriate material or messages or anything of an uncomfortable nature
- will only use academy systems and devices for educational use and not for personal or recreational activities unless permission has been specifically granted
- will not download or upload any data or store any files on the academy network or on academy hardware unless permission has been specifically granted
- will comply with all data storage, legal downloading, copyright and licencing requirements
- will not use the academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube)
- will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without staff permission

- will be polite and responsible when communicating with others. Students will not use intimidating, offensive or inappropriate language and will not post material of this nature at any time
- will not use personal devices - USB devices, mobile technologies eg IPads – in school unless permission has been specifically granted by a member of staff. In all cases, the requirements of this agreement must continue to be complied with
- will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- will not use any programmes, specialist software or hardware which might enable students to bypass the internet filtering/security systems in place to prevent access to such materials
- will immediately report any damage or faults involving equipment or software, however this may have happened
- will not install or attempt to install or store programmes of any type on any school device, nor attempt to alter any computer setting
- will not access or share any material of a pornographic, terrorist, extremist or violent nature or material which promotes discrimination, is sexually explicit or is in breach of any of the requirements set out in this policy, and the academy's policies on safeguarding and acceptable conduct
- will understand that the academy has the right to take action if students are found to be in breach of this agreement where academy systems may not be used but where they involve members of the school community (examples would be cyber-bullying, unauthorised use of images or personal information).

5. Compliance

Any failure to comply with the requirements of this agreement will result in sanctions being applied in line with the academy's behaviour policy. This may include loss of access to the school network/internet, contact with parents, exclusion and possibly the involvement of the police in the event of very serious non-compliance and/or illegal activity.

In accessing the academy's ICT systems, it will be assumed that all users are in agreement and will comply with the requirements of this policy.

4. Review History

Version	Date	Changes	Approval
1	November 2015	Revised and incorporates requirements of Prevent Agenda and E-Safety	Access Committee
2	November 2017	Minor amendments	Full Governing Body