E-SAFETY POLICY

Policy Ref	P06
Version	2
Originator	Janice Hamilton
Approved	14 November 2017 by CLT
Issue Date	November 2017
Review Date	Subject to changes in Trust policy

A Introduction

A.1 The College, as part of the Ninestiles Academy Trust, uses ICT to:

- Contribute to high quality teaching and learning
- Enable effective tracking, target setting and the management of intervention strategies
- Enable focused assessment
- Support effective internal and external communication.

A.2 However, there are inherent dangers of using this powerful took in an educational environment. It is therefore essential that the College and schools within the Trust create a safe ICT learning environment that includes three main elements:

- An effective range of technological tools
- Policies and procedures to describe and maintain the acceptable use of the Trust's ICT services and facilities with clear roles and responsibilities
- A comprehensive e-safety education programme for students and staff.

A.3 This E-Safety Policy has been written in accordance with our vision for the College and the Trust, and is supported by the following policies: Anti-Bullying Policy, Commitment and Student Disciplinary Processes, Complaints Policy, Student Enrolment Contract, Safeguarding & Child Protection Policy including Prevent, student and staff Acceptable Use of ICT guidelines, and Social Media Policy.

B Key Principles

B.1 All students should be able to learn in a safe environment and should not be exposed to inappropriate materials or cyber bullying.

B.2 All staff are responsible for promoting and supporting safe behaviours in their classrooms and following the College and Ninestiles Academy Trust's E-Safety Policy.

B.3 There is a "no blame" culture so students feel able to report any bullying, abuse or inappropriate materials for investigation.

C The aims of the policy are:

- To ensure students can learn in a safe and secure environment, in and out of the College.
- To minimise the risk of student exposure to inappropriate material or cyber bullying.
- To develop secure practice for students when communicating electronically.
- To develop student self-responsibility when communicating electronically.
- To ensure consistent good practice for staff when communicating electronically.
- To ensure all staff are aware of issues relating to e-safety.
- To provide information, advice and guidance on the use of new technologies.

D Roles and Responsibilities

D.1 Trust

- Ensure the E-Safety Policy is implemented, monitored and reviewed.

D.2 College

- Ensure, along with the Academy Council, that the E-Safety Policy is implemented, monitored and reviewed
- Ensure that all staff are aware of their responsibilities under this Policy and are given appropriate training and support so that they can fulfil their responsibilities
- Ensure that issues of e-safety, including cyber bullying, are addressed within the curriculum

D.3 College's Designated Safeguarding Lead

- Responsibility for e-safety in the College.

D.4 College ICT Support Team

- Ensure the College remains up to date with e-safety issues and guidance through organisations such as the Child Exploitation & Online Protection (CEOP)
- Ensure the Principal is updated as necessary, including being aware of local and national guidance on e-safety and updated at least annually on policy developments
- Ensure the College network is safe and secure for all groups – consistent application of protocols and management and development of software
- Advise Academy Council, College Leadership Team, teachers, technicians, and academic coaches on e-safety issues
- Take responsibility for promoting and supporting safe behaviours in classrooms and following College e-safety procedures.

E The College Network

E.1 The security of the College network is maintained by:

- Ensuring its health, through appropriate anti-virus software etc and network set-up so staff and students cannot download executable files such as .exe / .com / .vbs etc
- Ensuring it is 'healthy' through robust monitoring on the network (these may be replaced or updated as appropriate to take account of technical and commercial developments)
- Ensuring the ICT Services Manager is up to date with providers' services for security
- Ensuring that the filtering methods are effective in practice and that access to any website considered inappropriate by staff is removed immediately (responsibility of ICT Services Manager)
- Not allowing students access to internet logs
- Using individual log-ins for students and all other users
- Never sending personal data over the internet unless it is encrypted or otherwise secured, or sent via secure systems such as the DfE s2s site
- Ensuring students only publish within appropriately secure learning environments such as their own closed secure log-in.

F The Internet

F.1 The College and Ninestiles Academy Trust schools recognise that access to the internet is an invaluable learning tool and vital for effective communication. Safety and security risks are minimised through:

- The use of internal filtering systems which block sites that fall into categories such as pornography, race hatred, gaming, other sites of an illegal nature
- Effective planning – internet use is matched to students' abilities
- Informing users that internet use is monitored at in the Acceptable Use Policy, and as part of the student induction process in ICT lessons
- Informing staff and students that they must report any failure of the filtering systems directly to a member of staff
- Blocking all chatrooms and social networking sites except those that are part of an education network
- Only using approving blogging or discussion sites
- Requiring all staff to be aware of the Acceptable Use Policy and that on signing their terms and conditions of employment they agree to comply with its contents
- Ensuring all users know and understand what the rules of appropriate use are and what sanctions result from misuse – through induction (refer to the internet and email policies)
- Maintaining a record of any cyber bullying or inappropriate behaviour (the bullying log and safeguarding record) and act to deal with the perpetrators of such behaviour
- Making information on reporting offensive materials, abuse, bullying etc available for students, staff and parents
- Immediately referring any material suspected of being illegal to the Police

- Establishing that email and internet use is not private and the College reserves the right to monitor all emails and internet usage involving the College's IT facilities and/or services This will include personal devices when connected to the College IT services, but will be limited to the usage of those services.
- Allocating an email account through the College domain, enabling them to access their email from College and at home through the College Gateway page.
- Ensuring staff do not communicate with students via their personal email accounts, communicate through their personal social networking site account or give access to information or data via personal cloud accounts.
- Ensuring staff only communicate with students via their designated College email account or Tyber
- Ensuring staff do not attempt to use their personal social networking site(s) in College
- Ensuring staff do not communicate with or have details of students on their personal social networking account or any other electronic device, eg Facebook
- Ensuring that staff do not have student contact details on their personal mobile phones, except for the specific duration of a College trip/visit
- Ensuring that student details are always taken from Tyber and any new contact details obtained are passed to MIS for updating records as appropriate
- Making students aware of the risks and issues associated with communicating through email and to have strategies to deal with inappropriate emails, as part of the College's e-safety and anti-bullying education programme.

G Digital and Video Images

G.1 To prevent the inappropriate use of images of students within the College, the following is observed:

- Notification is given to students that the College may publish photographs, video footage etc of students but will ensure that images may be used only to represent the College or the Ninestiles Academy Trust
- If photographs are published on the internet, in press releases or in case studies for example, full names may be used with the consent of the students involved
- Digital images/videos of students are stored securely
- Students' names are not used when saving images in the file names or in the <ALT> tags when publishing on the College website
- The College avoids including the full names of students in the credits of any published video materials/DVDs, or anywhere they can be easily identified from photos/videos
- The Principal takes overall editorial responsibility for the College website but delegates the operational day-to-day management to a named individual to ensure content is accurate and quality of presentation is maintained
- Uploading of information is delegated to individuals responsible for specified areas
- The College website complies with Ofsted guidelines
- Where other's work is published or linked to, the College credits the sources used and states clearly the author's identity or status

- The point of contact on the website is the main College address and telephone number. Home information or individual private email identities will not be published
- Staff are made aware of the Acceptable Use policy and the Social Media Policy in induction and on signing the terms of conditions of employment are agreeing to comply with the policy.
- Students are taught to be aware of the possible wide range of audiences and how images can be abused.

H Cyber Bullying

H.1 The use of the internet, text messages, email, video or audio to bully a student or member of staff will not be tolerated. Bullying can be done verbally, in text or images, eg graffiti, text messaging, email or postings on websites.

H.2 Cyber bullying is a form of bullying via communication technology like text messages, emails or websites. It takes many forms: sending threatening or abusive text messages or emails, personally or anonymously; making insulting comments about someone on a website, social networking site (eg Facebook) or online diary (blog/Twitter); making or sharing derogatory or embarrassing videos of someone via devices or email.

H.3 The use of ICT to bully could be against the law. Abusive language or images used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous and contrive the Harassment Act 1997 or the Telecommunications Act 1984.

J Monitoring Arrangements

J.1 The College will aim to ensure that all appropriate monitoring arrangements in relation to all internet, email and related services and facilities that it provides are in place and the College will apply these monitoring arrangements to all users. These arrangements may include checking the content of, and in some instances recording, email messages for the purpose of:

- Establishing the existence of facts relevant to the College and the Trust
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of email facilities
- Ensuring effective operation of email facilities
- Determining if communications are relevant to the College, for example where an employee or student is off sick or on holiday.

J.2 The College may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of this policy.

J.3 These monitoring arrangements will operate on a continual and continuing basis, with the express aim of monitoring compliance with the provisions of the College's E-Safety Policy and for the purposes outlined above as permitted by the

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

J.4 The College may arrange for an appropriate disclaimer to be appended to all email messages that are went to external addresses from the College in order to provide necessary legal protection.

K E-Safety Education

K.1 Students

An e-safety programme is provided for all students at induction and includes how to stay safe, social media and cyber bullying. All students have to sign electronically to say they have read and understood the Acceptable Use of ICT guidelines.

K.2 Staff

As part of their induction, all new staff are required to read the E-Safety Policy, the Acceptable Use Policy and the Social Media Policy. All staff are required to read updated policies.

L E-Safety Complaints

L.1 Complaints are dealt with in accordance with the Complaints Procedure. Complaints of cyber bullying are dealt with in accordance with the Anti-Bullying Policy and within the Commitment and Student Disciplinary processes. Complaints related to child protection are dealt with in accordance with the College's Safeguarding & Child Protection Policy including Prevent.

L.2 The College takes all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a College computer or mobile device. The College cannot accept liability for material accessed, or any consequences of internet access or ICT usage.

L.3 The College will investigate a complaint received from both internal and external sources about any unacceptable use of ICT that involves the College's ICT facilities. An external complaint will be addressed with reference to the College's Complaints Procedure.

L.4 The investigation of facts of a technical nature, eg to determine the source of an offending email message, will be undertaken by the College's ICT Services Manager and Ninestiles Academy Trust's Network Manager in conjunction with other departments as appropriate.

L.5 Where there is evidence of a criminal offence, consideration will be given to whether the issue will be reported to the Police for appropriate action to be taken. The College will cooperate with the Police and other appropriate external agencies as required in the investigation of alleged offences.

L.6 In the event that the investigation of the complaint establishes that there has been a breach of the standards of acceptable use, then appropriate action will be

taken. The College will act promptly to prevent continuance or repetition of the breach, for example by withdrawal of any unacceptable materials. This action will be taken in accordance with the normal managerial arrangements, and will typically involve liaison between the appropriate member of the College Leadership Team and the ICT Services Manager.

L.7 Indications of non-compliance with the provisions of the E-Safety Policy will be investigated, as appropriate, in accordance with the provisions of the College's Disciplinary Procedures, as applicable to staff and students. Subject to the findings of any such investigation, non-compliance with the provisions of the E-Safety Policy will lead to appropriate disciplinary action, which could include dismissal on the grounds of gross misconduct for staff or exclusion for a student. Furthermore, publication, accessing or storing of some materials may not only amount to a disciplinary offence but also a criminal offence, in which case the issue will be reported to the Police for appropriate action to be taken.

L.8 Complaints of cyber bullying will be recorded and dealt with in accordance with the College's Anti-Bullying Policy.

L.9 Complaints related to child protection will be dealt with in accordance with the College's Safeguarding & Child Protection Policy including Prevent.

L.10 In the case of child pornography being found, the person suspected should be immediately suspended and the Police called on 0808 100 00 40.

L.11 Anyone may report any inappropriate or potential illegal activity or abuse with or towards a child online to Child Exploitation & Online Protection (CEOP) at http://www.ceop.gov.uk/reporting_abuse.html

M Links to other Policies

Acceptable Use Policy
Anti-Bullying Policy
Commitment and Student Disciplinary Processes
Safeguarding & Child Protection Policy including Prevent
Complaints Procedure
Student Enrolment Contract
Student and Staff Acceptable Use of ICT Guidance
Social Media Policy