Hayes School
(Part of the Impact Multi Academy Trust)

Policy Document

Policy Name: E-Safety Policy
Date of Last Review: Summer 2018
Date of Next Review: Spring 2019
SLT Responsible: Principal
E-Safety Policy

Contents

1. Introduction
   1.1 Policy Aims
   1.2 Writing and reviewing the E-Safety policy

2. Teaching and learning
   2.1 Why the Internet and digital communications are important
   2.2 Students will be taught how to evaluate internet content

3. Managing Internet Access, e-mail and website content
   3.1 Information system security
   3.2 E-mail
   3.3 Published content and Hayes School web site
   3.4 Publishing students’ images and work
   3.5 Social networking, personal publishing and password security

4. Managing filtering

5. Managing videoconferencing

6. Managing emerging technologies

7. Protecting personal data

8. Policy Decisions
   8.1 Authorising Internet access
   8.2 Assessing risks
   8.3 Handling e-safety complaints

9. Communicating E-Safety
   9.1 Introducing the E-Safety policy to students
   9.2 Staff and the E-Safety policy
   9.3 Enlisting parents’ and carers’ support

APPENDIX A: SOCIAL MEDIA AND NETWORKING GUIDELINES FOR HAYES SCHOOL STAFF
APPENDIX B: Glossary of terms and abbreviations used
1. INTRODUCTION

1.1 Policy Aims
Hayes School believes that the use of information and communication technologies in school brings great benefits. Recognising the e-safety issues and planning accordingly will help to ensure appropriate, effective and safe use of electronic communications.

This document also sets out the school’s policy on social media and networking. New technologies are an integral part of our lives and are widespread powerful tools which bring new communication opportunities in teaching and learning for the school staff in many ways.

This policy together with the Anti-Bullying, IT User Policy, Child Protection and Safeguarding Policy, Staff Code or Conduct and Staff Discipline Policy is designed to keep staff and students safe in school when using ICT.

1.2 Writing and reviewing the E-safety policy
The E-Safety Policy relates to other policies including those for ICT, bullying, safeguarding and child protection. We will review this policy every year.

Hayes School’s nominated E-Safety coordinator is Mr S. Addison who will liaise with Hayes School’s Designated Safeguarding Lead Officer, Mrs K. Sirett over cases of e-safety concern.

2. Teaching and Learning

2.1 Why the Internet and digital communications are important
- The Internet is an essential element in 21st century life for education, business and social interaction. Hayes School has a duty to provide students with high-quality internet access as part of their learning experience. Internet use will enhance and extend learning.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

2.2 Students will be taught how to evaluate internet content
- Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. This is evidenced in schemes of work in the ICT department.
- Hayes School internet access is designed expressly for student use and includes filtering appropriate to the age of students.
- Clear boundaries are set for the appropriate use of the internet and digital communications and are discussed with staff and students. Student education in e-safety takes the form of e-safety lessons in ICT and assemblies. Staff education takes the form of briefings and directing staff to the staff handbook for guidance. Parents are also informed of E-Safety at specific times throughout the year and through the newsletter.
• Students are educated through curriculum areas in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

• Online safety presentations take place every year for students and new students in Years 7 and 12 and parents/carers receive external training for an outside provider. The school informs and educates students on the following online safety issues and the actions they can take to protect themselves and report issues:

  (i) Inappropriate content: risks of being exposed to illegal, inappropriate or harmful material and methods for reporting such content;
  (ii) Contact: the risk of being subjected to harmful online interaction with other users.
  (iii) Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

3. Managing Internet Access, e-mail and website content

3.1 Information system security
• Hayes School ICT system security is reviewed regularly. We use a range of products to protect the system. These include: Anti-Virus software, and a firewall on the servers. We also use a Proxy Server (Lightspeed) that filters our internet traffic and allows IT services staff to track inappropriate internet usage by staff and students.

• The virus protection (Forefront) is installed on all machines and servers. It downloads updates once a day at 7am and sends them to the client machines after it has been downloaded. Forefront scans the clients every Wednesday at 12.30pm.

3.2 E-mail
• All of the below is explicitly taught in ICT lessons and through ICT based assemblies.

• At present students are provided with a school based Outlook e-mail account, giving them email and website access account. Students in Years 7-11 can only send internal emails to teachers and fellow students. Students in the sixth form are able to send emails to external addresses.

• Students do not have system permissions to set up groups in Outlook for conversations.

• Students should immediately inform a member of staff if they receive offensive/inappropriate e-mail. Staff should inform their line manager.

• In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

• Staff and students should only open emails from people they know and attachments should not be opened unless the author is known.
3.3 Published content and Hayes School web site

- Staff email addresses are published on the school website. No student personal contact information will be published on Hayes School website. External email contact with Hayes School is made through the postmaster@hayes.bromley.sch.uk email account. This account is administered by the Principal’s PA.

- The Webmaster Mrs C. Harney has overall editorial responsibility and ensures that published content is accurate and appropriate.

3.4 Publishing students’ images and work

- Photographs that include students are selected carefully.

- Students’ full names are not used anywhere on a school web site in association with photographs.

- Written permission from parents or carers is obtained before photographs of all students are published on Hayes School Web site. This takes the form of a consent form filled in by parents when students join Hayes School. This information is recorded on Hayes School’s management information system (SIMs). The school webmaster needs to be aware of this and cross reference to any pictures on website.

- Work can only be published with the permission of the student.

3.5 Social networking, personal publishing and password security (see Appendix A for Social Media and Networking Guidelines for Hayes School Staff)

- Hayes School controls access to social networking sites, and considers how to educate students in their safe use.

- Hayes School allows access to ‘Yammer’ – an enterprise social networking site which is part of the schools SharePoint visual learning environment. Yammer access is monitored by IT services with group conversations being screened regularly for offensive or inappropriate content. Students are not allowed to create groups on Yammer and a staff member must be a member of any Yammer groups that are created. New groups are checked on a regular basis by IT services. Students who misuse Yammer will have their accounts suspended and any other relevant behaviour sanctions appropriate for the misuse.

- Newsgroups will be blocked unless a specific use is approved.

- Students are advised never to give out personal details of any kind which may identify them, their friends or their location.

- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future. Students should only invite known friends and deny access to others.

- Students are advised on user account security and how to set strong passwords (9 characters long, including a mix of upper and lower case & numbers).
• Students are advised to let their parents, carers, teachers, police or responsible adult know if they are uncomfortable about any contact made on social networking sites or over the internet.

• Parents are educated about how to deal with e-safety during parent information evenings. Resources such as “know it all” CD and leaflets are routinely handed out during these evenings.

• Teachers should not become a “friend” of current students on social networking sites and should not communicate with students over the internet. Staff should only contact students using their school e-mail account for work purposes/school business in accordance with the Staff Code of Conduct.

• Use of school Twitter accounts - e.g. setting up and use of school Twitter accounts to communicate with students such as the Drama Department Twitter feed must be approved by the Principal. Communications will be regularly monitored by the E-Safety co-ordinator.

4. Managing Filtering

• Hayes School works in partnership with Class Technology Solutions (CTS), our network provider and other schools, as appropriate to ensure that systems to protect students are reviewed and improved.

• If staff or students discover an unsuitable site, it must be reported to the classroom teacher who will inform the E-Safety Coordinator and/or IT Services who will block the site.

• IT services staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

• E-Safety software has now been installed across the school (Securus). This monitors all activity on the computers, across many categories including e-bullying, language, inappropriate content and activities.

5. Managing Videoconferencing

• All videoconferencing uses (Voice over Internet Protocol) VoIP specifically Skype.

• Students are not given access to VoIP. Teachers always lead VoIP sessions.

6. Managing Emerging Technologies

• Emerging technologies are examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.

• Mobile phones are not to be used during lessons or inside Hayes School without the prior permission of the teacher. The sending of abusive or inappropriate text messages is forbidden.
and should such text messages be received students are encouraged to bring them to the attention of a member of staff so that appropriate action can be taken.

- The use by students of mobile phones may be permitted in lessons by a teacher to carry out research, use mobile applications or to photograph or film work under the close supervision of the teacher. Mobile phones should not under any circumstance be used to film/photograph students in lessons. Camcorders are available for this purpose from the Media Arts department.

- Staff members are to use Hayes School’s phone system to contact students and not their mobile phones.

- Staff should not use their personal phone camera/personal cameras to record student activity.

- The school recognises that many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school accordingly restricts the use of mobile phones to use at break and lunch outside the buildings. Parents/carers are advised by the school to ensure that appropriate filters are in place from their network provider.

7. Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998. (See the Data Protection Policy)

8. Policy Decisions

8.1 Authorising Internet access

- All staff must read and accept/acknowledge the ‘Staff ICT User Policy” when logging into the school network within school and remotely.

- Hayes School maintains a current record of all staff and students who are granted access to school ICT systems.

- Students must comply with the Acceptable Use Policy in their planners. This must be signed by both students and parents at the beginning of each year. ICT teaching staff are to ensure this is completed for all their classes.

- Students are allowed access to their user areas from home. The same acceptable use policy applies at home as in school.

8.2 Assessing risks

- Hayes School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to Hayes School network. Hayes School cannot accept liability for any material accessed, or any consequences of Internet access.
Hayes School
(Part of the Impact Multi Academy Trust)
E-Safety Policy

- Hayes School audits ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective.

- In line with the Child Protection & Safeguarding Policy staff should not store images of students on laptops or personal devices.

8.3 Handling e-safety complaints
- Complaints of internet misuse will be dealt with in the first instance by the Network Manager who may refer it to a relevant senior member of staff.

- Any complaint about staff misuse must be referred to the Principal.

- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.

- Complaints of a bullying nature will be dealt with in accordance with both the child protection and safeguarding procedures, anti-bullying policy and behaviour management.

9. Communicating E-Safety

9.1 Introducing the E-Safety policy to students
- E-Safety rules will be posted in all rooms where computers are used.

- Students will be informed that network and internet use is monitored.

- A programme of training in E-Safety has been developed, and is led by the ICT teaching team through lessons and assemblies supported by CEOP.

- The school website contains a link to e-safety resources.

- In Spring Term 2015 all students in Years 7-12 received e-safety awareness training provided by Education Child Protection Limited.

9.2 Staff and the E-Safety policy
- All staff have access to the Hayes School E-Safety Policy, and its importance is explained.

- Staff are informed that their account and activities on the user account including the internet can be monitored and traced to the individual user.

- Staff that manage filtering systems or monitor ICT use clear procedures for reporting issues.

- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship. When communicating with a student via electronic means, staff must always CC their line manager into the communication.
• When staff are in email communication with parents they should always CC their line manager into the email.

• Staff should not have images of students on mobile phones, staff personal cameras or on home computers.

9.3 Enlisting parents and carers support
• Parents and carers attention will be drawn to Hayes School E-Safety Policy in newsletters and on the Hayes School website. This will include a list of e-safety resources, information and guidance for parents/carers from other organisations e.g. NSPCC, CEOP

• E-safety awareness training provided by Education Child Protection Limited is planned for parents in 2016-17. A parent’s session took place in autumn 2015.

APPENDIX A. SOCIAL MEDIA AND NETWORKING GUIDELINES FOR HAYES SCHOOL STAFF

1. Introduction

(i) This document sets out the school’s policy on social media and networking. New technologies are an integral part of our lives and are widespread powerful tools which bring new communication opportunities in teaching and learning for the school staff in many ways. It is important that we are able to use these technologies and services effectively but that this should be balanced with protecting our professional reputation and integrity. With this in mind, all staff working with students have a responsibility to maintain public confidence in their ability to safeguard their welfare, and to behave in the best interests of the students and the school. These guidelines are also designed to protect staff from possible harassment by a colleague or student via a social networking site.

(ii) These guidelines should be read in conjunction with the school’s Child Protection and Safeguarding Policy, Staff Code or Conduct and Staff Discipline Policy. If staff fail to adhere to the guidelines set out, their conduct could be called into question and this may result in disciplinary action being taken against them which could ultimately lead to their dismissal.

(iii) Whilst these guidelines have attempted to cover a wide range of situations, they cannot cover all eventualities. Staff using social media and networking sites should avoid any conduct which would lead any reasonable person to question their motives and intentions.

(iv) The school understands that employees have the right to a private life and would respect this so long as employees follow the guidelines set out in this document and other documents they refer to. The school expects employees to maintain reasonable standards in their own behaviour such that enable them to maintain an effective learning environment and also to uphold public trust and confidence in them and their profession. Employees should avoid any conduct which is likely to bring the school into disrepute.
2. Scope

(i) This document applies to all staff who work in the school. This includes all teaching and non-teaching staff. The general principles set out should also be followed by adults who work at the school but are not employed by the school.

(ii) For the purpose of these guidelines, social media and social networking sites are websites by which personal information or opinions can be presented for public consumption and websites which allow people to interact with each other. Examples of social media and social networking sites could be all internet presence including blogs, Facebook, Twitter, Web 2, Bebo, Youtube and MySpace. Please note that this list is not exhaustive as new technology is emerging on a daily basis but it seeks to provide examples to staff. The definition of social networking and media may be increased as new technologies emerge.

3. Staff guidelines in relation to social networking and media activity

(i) If you wish to have a social media presence, please make sure that your employer is not identified on this presence unless there is, on an objective assessment, a legitimate reason for doing so and ensure that comments made are from your own behalf, for example by writing in the first person and using a personal email address as opposed to your employer’s email address.

(ii) Staff are personally responsible for their communication in social media. This includes any media attachments like photographs or videos. What staff publish on a social media site will be available for any member of the public to read (including parents, members of the Governing Body, colleagues, members of the Local Authority and prospective employers) for a long time. Staff should always think carefully about this when posting personal content.

(iii) Staff should not post any media attachments such as photographs or videos which have subjects (students/colleagues etc.) of the school in them. If you wish to post such items you should always speak to the Principal in the first instance.

(iv) Staff should not place any information regarding their employer, their colleagues, students or people they come into contact with as part of their employment on a social networking or media site.

(v) Staff are advised for their own protection not to put personal information such as home addresses or personal telephone numbers on a social networking or media site.

4. Staff guidelines in relation to student contact

(i) Staff are not expected to interact with any student (or past student under the age of 18) of the school on a social media or networking site. For example, the school would
not think it appropriate for staff to ‘friend’ a student or request that a student ‘friend’ them.

(ii) Any electronic communication regarding the school or the work you are carrying out in the school (including telephone and text messaging contact) with students or parents/carers should only take place using the school’s formal communication systems. Staff should only use the school’s website; the school’s email address or the school’s telephone number when communicating with students and parents/carers.

(iii) Staff should not post remarks or comments on-line or engage in online activities which may bring the school into disrepute.

5. **Social media and networking sites and cyberbullying**

(i) Staff should never use social media to abuse or bully or otherwise comment about colleagues, students, carers of the students or anyone associated in the wide context of the school (e.g. member of the Governing Body, Local Authority, sponsor etc.). Staff are expected to act respectfully when using social media and to avoid language which may be deemed as offensive to other people. For example, the school would not expect to:

- post anything that could be construed as discriminatory
- post anything that could be construed as racist
- post anything that is untrue or misleading
- post anything that engages in criminal activity
- post anything that is defamatory about people or organisations

(ii) Staff who feel that they are subject to social media bullying by another member of staff or a student should where possible save evidence (e.g. emails, screen prints, text messages) and immediately report this to the Principal for further investigation. Where the complaint is against the Principal, the concern should be raised with the Chair of the Governing Body for further investigation.

(iii) Staff who feel that a colleague is not adhering to these guidelines should report their concerns to the Principal for further investigation. Where the complaint is against the Principal, the concern should be raised with the Chair of the Governing Body for further investigation.
APPENDIX B: Glossary of terms and abbreviations used

1. CEOP: Child Exploitation and Online Protection is a command of the UK’s National Crime Agency, and is tasked to work both nationally and internationally with keeping children safe online.
2. CTS: Class technology Solutions are the company which currently provide the school’s ICT network support.
3. Forefront: Anti-virus software installed on machines and servers within school to ensure the network is protected from viruses, spyware and malware.
4. ICT – Information and Communications Technology
5. Lightspeed: This is a proxy server which filters internet access to prevent inappropriate material being seen in school and monitors web activity of all school users on the school network (both wireless and wired internet use)
6. NSPCC: National Society for the Prevention of Cruelty to Children, this is a charity based in the UK which works to keep children safe
7. Securus: Software which monitors language and activity online and it able to detect and flag the use inappropriate language or content to the school’s ICT support team.
8. SIMs: The school’s database containing records of colleague, student and parent details.
10. Yammer: an enterprise social networking site which is part of the schools SharePoint visual learning environment. This can only be accessed by Hayes students and colleagues.