e-Safety and IT Acceptable Use Policy

Owner:	Network Manager
Document No:	IT/CD/002
Version:	V1
Last Review:	July 2016
Review Agreed by:	Head of Estates & IT
Last Approved:	22 September 2016
Approved by:	Pending Corporation
Next Review:	July 2018
Related Documents:	Safeguarding Policy Child Protection and Vulnerable Adults Safeguarding Policy and Procedure Safeguarding Professional Practice and Boundaries Policy Safeguarding Guidance for Safer Working Practice for Staff Working with Young People and 'At Risk' Adults Data Protection Policy CCTV Policy Equality and Diversity Policy

Contents

1.0 Introduction 3
2.0 Scope of Policy 3
3.0 Legislative Requirements....3
4.0 Prevent Duty 3
5.0 General Responsibilities, Operating Principles and Personal Use 4
6.0 Monitoring of College IT Systems 6
7.0 Use of Email 8
8.0 Use of Internet, Social Media and Social Networking Sites 10
9.0 Copyright, Downloading and Data Storage....13
10.0 Use of Personal Devices on the College Network 13
11.0 Staff Use of Telephones and Other Mobile Devices or Services 14
12.0 Misuse of this Policy 17
13.0 Policy Review 17
Appendix 1: Equality Impact Assessment....18

1.0 Introduction

1.1 This Policy reflects Havering College's commitment to maintaining e-safety and acceptable use of its IT systems by staff and students. It identifies the duties and responsibilities of all users of College IT systems and provides guidance on actions to be taken to ensure compliance.

1.2 The College invests substantially in email and internet systems and the facilities provided represent a considerable commitment of resources. This Policy informs staff and students of the College's expectations for the appropriate use of those resources.

1.3 In addition, the College is aware of the accessible and global nature of the internet, email and related technologies that are available along with the potential risks and challenges associated with their use. The College manages these through the implementation of security measures and safeguards within the IT systems, and by supporting staff and students to identify and manage risks independently.

1.4 Havering College staff and students must comply with the requirements of this Policy.

2.0 Scope of Policy

2.1 This Policy relates to all Havering College IT systems and is relevant to all staff, students and any other persons who may have cause to use them.

2.2 In particular the scope of this Policy covers the responsible and appropriate use of College IT Systems including operating principles and personal use; system monitoring; emails; internet and social media; copyright, downloading and data storage; personal devices; and telephones and other mobile devices.

3.0 Legislative Requirements

3.1 The College will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which is predominantly the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Data Protection Act 1998; the Human Rights Act 1998; and the Education Act 2011.

3.2 In addition the College has a statutory and moral duty to ensure that it functions with a view to safeguarding and promoting the welfare of children and vulnerable adults receiving education and training at the College. Consequently, the College will do all that is reasonably possible to keep students and staff safe online and to satisfy the College's wider duty of care.

4.0 Prevent Duty

4.1 Prevent is a Government led strategy that aims to stop people being drawn into terrorism or supporting terrorism.

4.2 The internet has transformed the extent to which organisations and their sympathisers can radicalise people in this country and overseas. It enables a wider range of organisations and individuals to reach a much larger audience with a broader and more dynamic series of messages and narratives. It also encourages interaction and facilitates recruitment. The College has recognised that there are a number of specific measures which it can take to address the threat of radicalisation online. They include steps to:

- Restrict access by College users to harmful content online through the use of internet filtering and monitoring;
- Ensure appropriate action is taken against anyone found to be knowingly attempting to access unlawful and harmful content from the internet;
- Educate users at risk and encourage programmes led by the local police forces, communities and local authorities to raise awareness to all College internet users.

4.3 Further information relating to 'Prevent' can be sourced from the College Safeguarding Policy or by contacting the Safeguarding, Prevent and Operations Officer.

5.0 General Responsibilities, Operating Principles and Personal Use

5.1 All Users

5.1.1 The College IT systems including computers, email and internet are primarily for business use by staff and for the purposes of learning for students.

5.1.2 Each user is issued with a unique password for use of the College computer systems, for security purposes. Staff and students are responsible for protecting their password. For reasons of security, users must not print, store online or share their individual passwords with others. Users are required to change their password periodically and will be prompted to do so by an automated policy.

5.1.3 Users must not attempt to defeat, circumvent or bypass any of the College internet or computer security systems or attempt to access College systems using somebody else's security/password details.

5.1.4 User must not connect any personal laptop, tablet, smartphone or other mobile device to the College network using a network cable or download or install any software on to College computers or devices.

5.1.5 The College recognises that in certain circumstances, particularly when there is a need to communicate urgently, it may be appropriate for staff or students to send and receive personal emails. Therefore, the College permits the occasional use of internet and email systems to send personal emails and browse the internet but such reasonable private usage of email and internet must not interfere with work or learning activities. However, such limited personal usage must still adhere to the standards outlined in this Policy. Consequently, excessive private use for non-business or learning purposes will be dealt with under Havering College's Disciplinary Policy for staff or the Student Disciplinary Procedures for students and in certain circumstances may be treated as gross misconduct.

5.1.6 In the interests of personal safety, respect and the protection of others, users:

- Should not give out their name, phone number, address or other personal details over the internet.
- Must not use offensive websites and all internet posts and emails must be sensible and non-offensive.
- Must not take or use photographs or films of people at the College, or learners outside of the College, without their permission.

5.1.7 The ability for users to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless they are authorised to do so. Users should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file except where a file is on a shared drive/shared area and the users has specific access to that shared drive/shared area.

5.2 **Havering College Staff**

5.2.1 Staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this Policy. Staff who have been issued with a laptop, tablet, smartphone or other mobile device must ensure that it is kept secure at all times and that it is password protected, especially when travelling. Staff should be aware that if using equipment on, for example, public transport, it may be possible for documents to be read by others so vigilance must be maintained at all times.

5.2.2 The IT Team are responsible for maintaining the College's computer systems and for supporting staff and students in the proper use of the systems. Where staff require any information or help about the use or set up of the computer facilities, queries should be directed to the IT Helpdesk.

5.2.3 All staff must undertake Prevent and safeguarding training provided by the College to ensure they remain aware of their duties in this regard.

5.2.4 All staff are responsible for ensuring the safety of students. Any e-safety incidents should be reported using the procedures outlined in the College's suite of safeguarding policies.

5.2.5 The Principal is responsible for overseeing all matters concerning safeguarding. The Safeguarding/Prevent and Operations Officer within Student Services and the Director of Human Resources are the nominated Child Protection/Safeguarding Officers. Where a safeguarding incident may include e-safety, the Safeguarding Officers may consult with the Police Liaison & Premises Support Officer, the Premises Supervisor, the Head of Estates & IT, or one of the College senior post holders these being the Principal, the Vice Principal or the Director of Finance and Corporate Affairs.

5.2.6 Personal Tutors and/or Progress Coaches are responsible for facilitating e-safety sessions. In addition, it is the responsibility of all teaching staff to reinforce this message as part of the tutorial programme and to read through and adhere to the incident reporting procedure as contained in the Safeguarding Policy. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

5.2.7 Where management considers it appropriate, the Safeguarding/Child Protection Officer may be asked to intervene with appropriate additional support from external agencies.

5.3 **Havering College Students**

5.3.1 All students will receive e-safety lessons from support or teaching staff and must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their Personal Tutor/Progress Coach or teaching staff.

5.3.2 Students are responsible for respecting the College IT systems and equipment allocated to or used by them in accordance with this Policy.

5.3.3 Access to the College IT systems is provided to students for the purposes of learning. However, it is permissible for students to use social networking sites in open-access IT areas but not in classrooms or the Learning Resource Centres (LRCs), unless this has been agreed by their tutor or a member of LRC staff.

5.3.4 Students may be permitted to use their own personal laptop, tablet, smartphone or other mobile device connected via wireless or cellular data in College classrooms if their tutor has agreed that they may do so.

5.3.5 Students must advise their tutor immediately if they see an offensive website or receive an email or message that causes them concern or distress.

5.3.6 Where students require any information or help about the use or set up of the computer facilities, queries should be directed to the IT Helpdesk.

6.0 Monitoring of College IT Systems

6.1 Computer and email accounts are the property of the College and are designed to assist staff and students in their work. Users of College IT systems should therefore have no expectation of privacy in any email sent or received, in the social media or other internet sites they access, or in respect of telephone or mobile device usage.

6.2 The College has rights to intercept email and monitor internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons:

- To establish the existence of facts relevant to the College's business;
- To ascertain compliance with regulatory practices or procedures relevant to the College;
- To ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties;
- In the interests of national security
- To prevent or detect crime;
- To investigate or detect the unauthorised use of internet and email systems;
- To ensure the effective operation of the system, e.g. to detect computer viruses and to maintain an adequate level of security

6.3 Consequently, the College monitors telephony systems, emails, and internet access and usage for business and security purposes and to ensure that staff and students make appropriate use of the systems at all times.

6.4 All internet activity through College IT systems is logged and the College considers that valid reasons for checking an employee's or students' internet usage logs include suspicions that they have:

- Been spending an excessive amount of time using social media websites for non-work-related activity; or
- Acted in a way that is in breach of the rules set out in this Policy

6.5 The College reserves the right to retain information that it has gathered on staff and student use of the internet for a period of one year. However, if information has been requested and provided as part of an investigation it is possible that it may be retained for longer than one year if there is an ongoing court case.

6.6 In addition to monitoring the content of all online communications over its networks, the College also monitors the content of secure sites, when this content is generated through student accessible IT equipment.

6.7 In the event of any investigation into an employee's computer activity all staff are treated the same except that if an employee is also a trade union representative then the College will inform a regional representative of that union of any such investigation that may take place.

6.8 Although an email that is clearly marked as private cannot be defined as a communication relevant to the College's business, the College reserves the right to monitor the content of such an email where there is a reasonable belief that it may breach this Policy, for example by containing discriminatory or pornographic material.

6.9 In order to meet business needs, the College may need to check the emails of staff that are absent. The College will endeavour to notify the member of staff concerned before undertaking the monitoring of emails in such circumstances.

6.10 To be able to exercise its rights (as described in point 6.2 above), the College must have made all reasonable efforts to inform every person who may use the email and internet systems that monitoring may take place. The College believes that the communication of this Policy to all staff and students meets this requirement and therefore asks all staff and students to confirm that they have read and understood this Policy when logging on to a College device or connecting to the College network for the first time. This process will also be repeated at the start of every academic year to remind staff and returning students of the Policy requirements.

6.11 The College reserves the right to use the content of any staff or student email in any disciplinary process and users should note that for a period of time all emails can be recovered even after they have been deleted. Emails are also disclosable in any litigation proceedings.

6.12 The College reserves the right to inspect any files stored by staff or students in private areas of the computer system to assure compliance with this Policy.

6.13 In addition, Closed Circuit Television (CCTV) is in operation internally and externally on all sites for the protection of staff and students. CCTV usage is covered in the College's CCTV Policy.

6.14 The College recognises the importance of working closely with its recognised trade unions and fully respects the views of trade union representatives in the event of a trade dispute. No trade union representative will normally be subject to any form of disciplinary action in respect of their views regarding any trade dispute provided always that the views are genuinely made in respect of that dispute and are not considered to be defamatory towards the College or any employee, officer, worker or student of the College.

7.0 Use of Email

7.1 By sending emails through the College IT system, users are consenting to the processing of any of their personal data contained in that email and are explicitly consenting to the processing of any of their sensitive personal data contained in that email. If staff or students do not wish the College to process such data, they should communicate that information by other means.

7.2 Emails should be drafted with care. Due to the informal nature of email, it can be easy to forget that it is a permanent form of written communication and that material can be recovered even when it has been deleted. Users should ensure that the content and tone of emails reflect the professional image of the College.

7.3 Emails should be clear and concise and should not be any longer than necessary and users should not send unnecessary emails, or copy other recipients into messages without good reason.

7.4 Users should not attach unnecessary files as large attachments can congest recipients' systems. File sizes greater than 20 Mb will not be processed.

7.5 Emails should not be written in capital letters as this can be construed as shouting via email.

7.6 In general, users must not send personal data of other persons or organisations via email, without the authorisation of the owners of that data.

7.7 Users must not send personal or confidential information and/or documents, or disclose confidential College information by email unless necessary and in accordance with the provisions of the Data Protection Act 1998. If it is necessary to share personal or confidential information via email then it must be securely marked **'Restricted'** within the email message subject line in accordance with the Government Protective Marking System (GPMS), which will ensure the email is encrypted. Failure to strictly comply with this requirement may lead to disciplinary action being taken in line with Havering College's Disciplinary Policy.

7.8 Emails must not contain any message or image that is discriminatory against any of the nine protected characteristics (on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex, or sexual orientation) of the Equality Act 2010, or which is, or constitutes obscene, pornographic, abusive, or threatening behaviour. The College does not tolerate discrimination, harassment or bullying and any breach of this rule may constitute gross misconduct.

7.9 Users should not make any derogatory remarks in emails. Written derogatory remarks could be considered to be defamatory, which could give rise to legal action being taken against the author and/or the College. Staff or students may also face disciplinary action in these circumstances as such conduct may constitute gross misconduct.

7.10 The College's email facilities must not be used to undertake illegal activity, including the display or sending of illegal material. Any such action may be considered as gross misconduct.

7.11 Users must not begin or distribute chain emails or other junk emails, including jokes and advertisements.

7.12 Users must be aware that a contractual commitment agreed by email may be binding and should therefore be entered into with due consideration. It is easy for email to be viewed as an informal means of communication, but commitments entered into in emails will have the same weight and status as any other written contracts.

7.13 Staff must never access another member of staff's email or network account; unless authorised by the Head of Estates & IT, the Director of Human Resources, the HR Manager, the Principal, the Vice Principal or the Director of Finance and Corporate Affairs. Access is permitted where a member of staff is absent from work and there is a business need for the College to check the emails of staff that are absent. In these circumstances the College will endeavour to notify the member of staff concerned before accessing their email or network account. When access is granted in such circumstances, staff must never send an email from that account; instead response emails should be sent from the individual's own College email account, clearly marked as being "on behalf of" the original recipient.

7.14 The following disclaimer must be, and is attached, to the end of every email sent externally (this is an automated process and is generated by College systems):

"This message is sent in confidence for the addressee only. It may contain confidential or sensitive information. The contents are not to be disclosed to anyone other than the addressee. Unauthorised recipients are requested to preserve this confidentiality and to advise us of any errors in transmission. Thank you.

Please note that the College reserves the right to monitor emails for the business purposes contained in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, that is: to establish the existence of facts relevant to the business of the College, to investigate or detect unauthorised use of the systems; to maintain the effective operation of the system; to detect any computer viruses; to check the mailbox of any absent employees; or to prevent or detect a crime. To be able to exercise these rights, the College must have made all reasonable attempts to inform every person who may use the system that monitoring and interception may take place. This College regards this notice to you as notification of such a possibility."

8.0 Use of Internet, Social Media and Social Networking Sites

8.1 Havering College recognises the growing significance of the internet and social media with regards to influencing public perception about the College, and its current and prospective students, staff and partners. Official College Facebook sites, College Twitter sites and YouTube accounts have been set up with the aims of informing stakeholders about College activities and developments, building online communities and facilitating stakeholders to share ideas and experiences through discussions, postings, photos and videos. Stakeholders include, but are not limited to, current and prospective students, College staff, alumni, partner institutions, governors, employers and members of the community.

8.2 Use of the internet, social media and social networking has become an essential and exciting part of everyday life. Millions of people use these platforms daily to view and share content online using websites and social forums such as Twitter, Facebook and LinkedIn. Social media also covers blogs, and video and image sharing websites such as YouTube and Flickr. However, there are a small minority of users who exploit social media to radicalise vulnerable people and users should be mindful of this when using them.

8.3 For the avoidance of doubt, when staff or students are using the internet, social media or social networking sites on College or other IT equipment and their use is linked to the College, then they are deemed to be representing the College. Examples of ways in which staff or students are linked to the College when they are using the internet are:

- Using a College email address as their contact email;
- Stating online that they work or study at Havering College;
- Posting comments about the College on social networking sites;
- Joining College staff or student networks on external websites;
- Using social networking sites to communicate with others in relation to College activities including work or study related matters.

8.4 Staff or students must not display, download, distribute, store, edit or record any material, including images, that are offensive, capable of constituting any form of discrimination, or which are obscene, pornographic, abusive, or threatening.

8.5 The College's internet facilities must not be used to undertake illegal activity, including the display, storage or downloading of illegal material.

8.6 Users must not download or distribute any pirated software using the College internet system.

8.7 The College's internet facilities must not be used to download entertainment software, including games, and users must not play games against other opponents or use gambling sites over the internet. However, this excludes the use of freely downloadable games software where it directly relates to teaching or coursework activity as part of the curriculum.

8.8 Staff or students must never engage in political discussions through outside newsgroups or any other means using the College's computer systems.

8.9 Staff and students should be aware that social networking websites are a public forum, particularly if they are part of a network. Users should not assume that their entries on any social media site will remain private, and should use the appropriate privacy settings to ensure their profile is protected and not open to the general public.

8.10 Users must also be security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth and place of birth which can form the basis of security questions and passwords. In addition, users should:

- Ensure that no information is made available that could provide a person with unauthorised access to the College, its systems and/or any confidential information; and
- Refrain from revealing any sensitive and/or confidential information regarding the College on any social networking website.

8.11 The College recognises that many staff and students make use of social media in a personal capacity. While they are not acting on behalf of the College, staff and students must be aware that they can damage the College reputation if they are recognised as being linked to the College. Therefore, any communications that staff or students make in a professional or personal capacity through social media, whether on College equipment or not, must not:

- Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by making offensive or derogatory comments, by using social media to bully another individual or by posting images that are discriminatory or offensive (or links to such content); or
- Bring the College into disrepute, for example by criticising or arguing with others, by making defamatory comments about individuals, other colleges or groups, or by posting images in links to content that are inappropriate
- Breach copyright, for example by using someone else's images or written content without permission or by failing to give acknowledgement where permission has been given to reproduce someone else’s work
- Make information available that could provide a person with unauthorised access to the College, its systems and/or any confidential information; and
- Reveal any sensitive and/or confidential information regarding the College on any social networking website.

8.12 Staff and students are reminded that they are legally liable for anything they write or present online. Users should also note that any breaches of this Policy may lead to disciplinary action. Serious breaches of this Policy, for example incidents of bullying or social media activity causing serious damage to the College, may constitute gross misconduct. In appropriate cases, in addition to disciplinary action, staff or students may be subject to civil or criminal proceedings.

8.13 Additional Guidance for College Staff

8.13.1 In addition to the reasons stated in point 8.11 above any communications that staff make in a professional or personal capacity through social media, whether on College equipment or not, must not:

- Do anything that could be considered a safeguarding issue as outlined in the College Safeguarding Professional Practice and Boundaries Policy; or
- Breach confidentiality, for example by revealing information owned by the College or by giving away confidential information about an individual or organisation; or
- Discuss the College's internal workings (such as deals that it is doing with a client or its future business plans that have not been communicated to the public)

8.13.2 Where staff use social media as a significant part of their curriculum and potentially contact students on a regular basis through social networking media their Assistant Principal must authorise the activity.

8.13.3 The College will retain the copyright to any material posted on the internet by a member of staff during the course of his or her duties.

8.13.4 Staff are permitted to make reasonable use of social media websites from the College's computers or devices, provided that this does not interfere with their duties or studies.

8.13.5 Whether using College computers or their own web-enabled devices, staff must limit their personal use of social media to their official rest breaks such as their lunch break/times.

8.13.6 Staff should not spend an excessive amount of time using social media websites whilst at work. Excessive use may lead to action under the College's Disciplinary Procedures and/or the withdrawal of an individual's access to IT facilities.

8.13.7 Access to particular social media websites will be withdrawn in any case of misuse.

8.13.8 Staff are allowed to say that they work for the College, which recognises that it is natural for them to sometimes want to discuss their work on social media. However, their online profile (for example, the name of a blog or a Twitter name) must not contain the College's name and if they do discuss their work on social media (for example, giving opinions on their specialism or the sector in which the College operates), they must include on their profile a statement along the following lines:

"The views I express here are mine alone and do not necessarily reflect the views of my employer."

9.0 Copyright, Downloading and Data Storage

9.1 Copyright applies to all text, pictures, video and sound, including those sent by email or on the internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

9.2 To protect the available bandwidth for all users, the ability to download high resolution images and multimedia files is limited and therefore at peak periods access to these resources is not guaranteed.

9.3 The College uses anti-virus programs on appropriate College IT systems. Where present, the anti-virus program will block access to downloadable content which contains viruses or malware, but such is the nature of viruses and malware that recent mutations may not be immediately detected by an anti-virus program. Therefore all staff and students should satisfy themselves whether the download is from a reliable source before it is run or accessed.

9.4 Users should not connect a non-College laptop or similar non-College device directly to the College's IT network using a cable. A secure Wi-fi network is available for this purpose.

9.5 **Additional Guidance for College Staff**

9.5.1 Staff are prohibited from downloading personal data of any sort from any College systems and storing such data on portable storage devices.

9.5.2 Staff are reminded that where personal data is generated by them, for example assessment scores or marks; these constitute personal data and must therefore be protected as such. A failure to comply with this obligation, which may expose the College to allegations of a breach of data protection, will result in disciplinary action and may in certain circumstances be treated as gross misconduct.

9.5.3 The College is able to provide staff access to software that can be used on personal devices for work-related purposes. If a member of staff subsequently leaves the College it is their responsibility to remove the software from their personal devices.

10.0 Use of Personal Devices on the College Network

10.1 This section is intended to address the use of non-College owned electronic devices in the workplace by staff and students. This includes smart phones, tablets and other such devices used to access College or non-College information.

10.1.1 The College requires that both students and staff conduct their online activities which concern the College appropriately and particularly in compliance with the terms of this e-Safety and IT Acceptable Use Policy. This requirement transcends whatever communications technology or device is being used.

10.2 **Usage**

10.2.1 Use of personal devices is at the discretion of the College and should not be seen as a right. Students' own devices can be used in the classroom at the teacher's discretion.

10.2.2 All personal devices shall only contact the internet and local area network via the College wireless network. All internet access via the network is logged and internet usage is monitored when connected to the College Wi-Fi network. The College will not monitor the content of user owned devices for threats to the technical infrastructure of the College but it reserves the right to prevent access to the College network by any device that is considered a risk to the network.

10.2.3 The use of cameras and recording equipment, including those which may be built in to certain devices, to make images or sound recordings of individuals, is prohibited unless with prior permission of any individual(s) being photographed/recorded.

10.2.4 The College does not approve any apps or updates that may be downloaded onto any device whilst using the College's wireless network and such activity is undertaken at the owner's risk, with the College having no liability for any consequent loss of data or damage to the individual's device.

10.2.5 All users are encouraged to protect their own devices using security passwords in place and that this security mechanism is used to protect that data. Students and staff are responsible for their own devices while on the College site.

10.3 **Security of College data**

10.3.1 When using a personal device to access the College systems and its data, you are expected to play your part in maintaining the security of College data and information that you handle. It is your responsibility to familiarise yourself with the device sufficiently in order to keep the data secure. In practice this means:

- Preventing theft and loss of data; and
- Where appropriate keeping information confidential; and
- Maintaining the integrity of data and information; and
- Never storing College data on a personal device

11.0 Staff Use of Telephones and Other Mobile Devices or Services

11.1 This section addresses the use of mobile devices or services provided by the College including mobile phones, smart phones, data modems, laptop computer, tablets and SIM cards.

11.2 **Use of Land Lines, Mobile Telephones, Smartphone and SIM card Use**

11.2.1 The Director of Finance and Corporate Affairs may, at their discretion, authorise the provision of a College mobile phone or smartphone to an employee who has a senior management role or whose role may involve child protection duties, or require them to respond to call outs, or respond to a critical incident (not including first aid).

11.2.2 The Director of Finance and Corporate Affairs may also, at their discretion, authorise the use of a College mobile phone or smartphone for an employee who spends more than two days per week away from a College campus on College business, or an employee whose role requires them to regularly move between College sites.

11.2.3 In order to qualify for consideration under 11.2.1 and 11.2.2 above, it will be essential for the employee or their line manager to demonstrate an ongoing business need and that without the use of a mobile phone:

- The employee would be unable to properly discharge their duties of employment; and
- The service provided by the College would be adversely affected.

11.2.4 Where an employee cannot demonstrate an ongoing business need, a 'pooled' mobile phone or smartphone may be provided on a short-term loan basis for those periods where there is a demonstrable business need.

11.2.5 Where an employee has the occasional need for a mobile phone for business use (e.g. invigilators, student trips), a Pay-As-You-Go (PAYG) mobile phone can be provided by the College on a short-term loan basis.

11.2.6 In all instances where mobile phones or smartphones are loaned on a short-term basis the following rules will apply:

- They must not be subject to any private use; and
- Any usage costs incurred by the College during the loan period or any costs for the loss, damage, repair or replacement of any device on loan will be recharged to the relevant department's non-pay budget

11.2.7 College owned mobile phone, along with its power-charger, SIM card, phone number and any other associated accessories, will remain the property of the College but the responsibility for the safekeeping and the proper use of the device will pass to the employee to whom they are issued. They must not be passed on to other employees without the written permission of the Estates and IT Department.

11.2.8 College owned mobile phone, smartphone or other SIM enabled device supplied to an employee is provided primarily for business use. The College accepts that there may be some incidental private use of such mobile devices (except those on short-term loan as per point 9.2.6 above) but this must not be significant.

11.2.9 In cases where private use of a mobile phone, smartphone or other SIM enabled device appears to be significant, the College will investigate the use and take appropriate action against the member of staff accordingly in line with Havering College's Disciplinary Policy.

11.2.10 Where private use is significant, a taxable benefit will arise on the relevant employee. The taxable benefit will be equivalent to the total cost to the College of providing the equipment to the employee and will include the total cost of both the line rental and all call charges.

11.2.11 Mobile phones, smartphones or other SIM enabled devices must not be used to make overseas voice calls. Except in cases of an emergency or where the call must be made out of normal College hours, such calls should be made using a College landline.

11.2.12 Where College mobile telephones, Smartphones or other SIM enabled device will be taken abroad on College business, the user must inform the Estates and IT Department before their departure. The Estates and IT Department will contact the mobile service provider in order to take advantage of any call plans or discounts which may apply to the countries being visited.

11.2.13 Making personal, external telephone calls (excluding calls in emergency situations) is not permitted using the College's land line telephone systems, unless the dialler accepts the call charges. Restrictions will also be set on the types of services available on selected telephones.

11.2.14 All landline calls are logged electronically. Management reports will be made available of numbers called and the duration of calls to clarify suspected misuse.

11.2.15 Telephone calls or texts to premium rate numbers are not permitted unless there are extenuating circumstances.

11.2.16 All handsets and mobile devices may be subject to password protection. Where passwords are used you should never reveal your password to other users once allocated.

11.2.17 A failure to comply with the College policy on telephone use will lead to disciplinary action and may in certain circumstances be treated as gross misconduct.

11.3 The Use of Mobile Devices whilst Driving

11.3.1 It is illegal to ride a motorcycle or drive a car while using a hand-held phone or any similar mobile device. This include whilst stopped at traffic lights, queuing in traffic or driving in a car park.

11.3.2 It is not illegal to use a mobile device via a hands free system whilst driving, but this can be a distraction. You will face the same penalties as using a hand-held mobile device if the police believe that you are not in proper control of your vehicle.

11.3.3 The College therefore regards the use of any mobile device whilst driving to be a danger to the driver, their passengers, other road users and pedestrians. Accordingly, the College discourages the use of any mobile devices, including via a hands free system, whilst driving.

11.3.4 Ideally all such devices should be switched off whilst driving. Any deviation from this Policy is at the drivers own risk and no responsibility will be accepted by the College for such actions.

11.3.5 Further guidance on this matter is available from the following web site: http://think.direct.gov.uk/mobile-phones.html.

11.4 **The Loss and Return of Mobile Devices**

11.4.1 All users of College mobile devices should take good care of those devices. The emphasis is on personal responsibility.

11.4.2 If a College device or a device containing College data is lost or stolen it must be reported immediately. Personal devices containing College data may be remotely wiped in these instances.

11.4.3 In the event that a user requires a replacement for a lost, stolen, or damaged College device they may be liable for the cost of replacement if it is considered that they have been careless or negligent in their actions. Subsequent and repeated losses may be viewed very seriously and could result in the College withdrawing the use of such devices from the employee, which may impact on their ability to conduct their duties and responsibilities of employment to the required standard.

11.4.4 All College owned mobile devices remain the property of the College and the College is responsible for all equipment costs and other contractual obligations. Therefore all mobile devices used by employees must be returned to the Estates and IT Department when leaving the employment of the College. Failure to do so will result in the full cost of replacement equipment being deducted from the final salary payment made to that employee.

11.4.5 Any redundant mobile devices should be returned to the Estates and IT Department.

11.5 **Use of Personal Mobile Devices**

11.5.1 Employees who use their own mobile devices in connection with College business may claim reimbursement in accordance with the College Expenses Policy.

12.0 Misuse of this Policy

12.1 Any misuse or breach of this Policy may lead to action being taken under Havering College's Disciplinary Policy for staff or the Student Disciplinary Procedures for students.

13.0 Policy Review

13.1 It is the responsibility of the Head of Estates & IT with support from the Network Manager to monitor and review this Policy, and to present any necessary changes, to the College Senior Leadership Team (SLT) and the Board of Governors.

13.2 This Policy will be reviewed every three years or in the event of any significant operational changes within the business, following a serious incident, or due to significant change in legislation.

Appendix 1: Equality Impact Assessment

EQUALITY IMPACT ASSESSMENT		
Lead Manager: Kevin Sullivan	**Area:** Estates and IT	
Policy/Service/Function to be Assessed:	e-Safety and IT Acceptable Use Policy	
New or Existing Policy/Service/Function?	○ New	◉ Existing
Which Stakeholders/Beneficiaries/Groups are intended to benefit from this policy/service/function?	All College Staff and Students	
1. Briefly describe the aims, objectives and purpose of this policy/service/function or area of work	This Policy is internded to ensure Havering College complies with its duties to ensure staff and students stay e-safe in line with safeguarding and Prevent requirements.	
2. Are there any other policies, procedures, guidance documents, services, functions, etc. that will interact with this policy/service/function?	Safeguarding Policy; Child Protection and Vulnerable Adults Safeguarding Policy and Procedure; Safeguarding Professional Practice and Boundaries Policy; Safeguarding Guidance for Safer Working Practice for Staff Working with Young People and 'At Risk' Adults; Data Protection Policy; CCTV Policy; and Equality and Diversity Policy	
3. Does the policy/service/function affect the employees including contract or agency workers?	◉ Yes	○ No
4. Does the policy/service/function affect the learners?	◉ Yes	○ No
5. Does the policy/service/function affect the public directly?	○ Yes	◉ No
6. Does the policy/service/function affect how other services are provided?	○ Yes	◉ No

7. What impact is the policy/service/function likely to have on the following protected characteristics:

(a) A **positive impact** is an impact that will improve equality of opportunity, have a positive impact on an equality group and/or improve relationships between members of different equality groups?

(b) A **negative impact** is an impact that could disadvantage one or more equality groups and/or have less beneficial outcomes for one or more groups when compared with another?

(c) A **neutral impact** is one where there is no disadvantage; experience will be the same for everyone?

(d) A **legal requirement** is where a negative impact can be justified on the basis of a legal requirement?

Protected characteristic	**Impact?**	**What data/evidence has informed the assessed impact and/or what initial action has been taken to deal with adverse or negative impact where practicable (further improvement measures can be added to the improvement plan at the end of this assessment where necessary)?**
Age	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.
Disability	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.
Gender	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.
Gender reassignment	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.
Marriage and civil partnership	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.

Pregnancy and maternity	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.
Race	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.
Religion or belief	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.
Sexual Orientation	NeutralNeutral	This Policy is aimed at the appropriate and safe use of IT systems by staff and students, hence it should have a neutral impact.

8. Consultation / Involvement:

(a) Who was consulted when the policy/service/function was written, amended or changed?	The purpose of this Policy is to ensure staff and students stay e-safe and in doing so help ensure safeguarding and welfare of College users. Consequently, consultation has not been undertaken with those who will be directly affected by this Policy as the purpose of this Policy is to help protect staff and learners of the College.
(b) What does available data and the results of any consultation show about the impact of this policy/service/function?	N/A

9. Are there any **staff development** and/or **training issues** on equalities arising from this assessment (included these in your improvement plan)	○ Yes ◉ No
10. How is the policy/service/function going to be **monitoring** in regards to how it affects the different equality groups?	This Policy is aimed at keeping staff and learners e-safe (as explained above) and hence this policy will only have a positive impact in this regard. Consequently, there is no intention to undertake regular checks on the affects of this Policy.
11. How is the policy/service/function going to be **communicated**?	This Policy is communicated at SLT level with a responsibility to cascade the policy to other levels of the College. In addition, all new starters (staff and students) at the College have to confirm that they have read and understood this Policy when logging on to a College device or connecting to the College network for the first time. This process is also repeated at the start of every academic year to remind staff and returning students of the Policy requirements.
12. Are there any further improvements that are required in relation to this Equality Impact Assessment? (included these in your improvement plan)	○ Yes ◉ No
Signed (Completing Officer): **(Completing Officer will implement this area of work)**	*Gerrard Shaw*
Print Name (Completing Officer):	Gerrard Shaw
Date:	15 July 2016
Signed (Lead Manager): **(Lead Manager is responsible for the effective working of this policy/service/function)**	*Kevin Sullivan*
Print Name (Completing Officer):	Kevin Sullivan
Date:	15 July 2016

EQUALITY IMPACT ASSESSMENT IMPROVEMENT PLAN					
Ref No.	**Improvement required**	**Timescale**	**Responsible**	**Date of completion**	**Signature**
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					