Norbury Manor Business & Enterprise College *for* Girls

E-safety Policy

Review date:	**May 2020**
Next review date:	**June 2021**
Staff resp. for review:	**TS**

Realising potential, nurturing leaders of the future

Norbury Manor Business and Enterprise College for Girls Internet/E-safety Policy Document

(to be read in conjunction with attached appendices)

This policy was written with the help and support of Kent Local Authority and London Grid for Learning (LGfL)

Context - why write an e-safety policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of college. It includes education for all members of the college community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Schools and other settings must decide on the right balance between controlling access to the Internet and technology, setting rules and boundaries and educating students and staff about responsible use.

Schools must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.

All members of staff need to be aware of the importance of good e-safety practice in the classroom in order to educate and protect the children in their care.

Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviour compatible with their role.

Breaches of an e-safety policy can and have led to civil, disciplinary and criminal action being taken against staff, students and members of the wider college community. It is crucial that all settings are aware of the offline consequences that online actions can have. Colleges must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Headteacher and the governing body.

The e-safety policy is essential in setting out how the college plans to develop and establish its e-safety approach and to identify core principles which all members of the college community need to be aware of and understand.

The e-safety policy should be used to develop an e-safety ethos and whole college approach.

In short:

- It is important to teach students about the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app

- However, schools also need an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their students

- Schools can refer to the Education for a Connected World Framework for age-specific advice about the online knowledge and skills that students should have the opportunity to develop at different stages of their lives

- When planning their curriculum, and how online safety fits within it, there are a number of areas we recommend schools consider, for example how to support vulnerable students

- We recommend that schools embed teaching about online safety and harms within a whole-school approach

Who will write and review the policy?

Our e–safety policy has been written by the college, building on the LGfL e–safety policy and government guidance; it has been agreed by the senior leadership team (SLT) and approved by governors.

- The e-safety policy and its implementation will be reviewed annually
- The college will appoint an e-safety coordinator who will work with the Designated Child Protection Coordinator as the two roles overlap
- Parents, students, staff and governors will be required to sign an e-safety/Internet acceptable use agreement as part of normal college procedures
- When staff, students and governors etc. leave the college their account or rights to specific college areas will be disabled

How does Internet use benefit education?

- Access to world-wide educational resources including museums and art galleries
- Access to experts in many fields for students and staff
- Access to learning wherever and whenever convenient
- Educational and cultural exchanges between students world-wide
- Vocational, social and leisure use in libraries, clubs and at home
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across networks of colleges, support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the local authority (LA) and Department for Education (DfE)

How can Internet use enhance learning?

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use

- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity
- Access levels will be reviewed to reflect the curriculum requirements and age of students
- The college will ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law

How will students learn how to evaluate Internet content?

- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of on-line materials is a part of teaching/learning in every subject

How will information systems security be maintained?

- The Network Manager will review system capacity regularly
- The security of the college information systems and users will be reviewed regularly
- The college's Internet access will be designed to enhance and extend education
- Files held on the college's network will be regularly checked
- Virus protection will be updated regularly
- Personal data sent over the Internet or taken off-site will be encrypted
- Unapproved software will not be allowed in staff or students' work areas or attached to email
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work

How will email be managed?

- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on the college's headed paper
- Access in college to external personal email accounts may be blocked in certain circumstances
- Staff should only use college email accounts to communicate with students as approved by the senior leadership team (SLT)
- Staff and governors should not use personal email accounts during college hours or for professional purposes
- Students may only use approved email accounts
- Students must immediately tell a teacher if they receive offensive email
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult
- Excessive social email use can interfere with learning and may be restricted
- The forwarding of chain messages is not permitted

How will published content be managed?

- The Headteacher has responsibility for the website and will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the college's guidelines for publications including respect for intellectual property rights and copyright
- Email addresses should be published carefully, to avoid being harvested for spam

Can students' images or work be published?

- When a student joins the school their consent is sought (see section 17 of the Data Protection Policy for details)

How will social networking, social media and personal publishing be managed?

- The college will block/filter access to social networking sites unless access is required for investigative purposes or for use in the classroom
- Teachers' official blogs should be password protected
- Teachers will be advised not to run social network spaces for student use on a personal basis
- Students will be advised never to give out personal details of any kind which may identify them and/or their location; examples would include real name, address, mobile or landline phone numbers, college attended, IM and email addresses, full names of friends, specific interests and clubs, etc.
- Students should be advised not to place personal photos on any social network space; they should consider how public the information is and consider using private areas; advice should be given regarding background detail in a photograph which could identify the student or his/her location, e.g. house number, street name or college
- Students should be advised on security and encouraged to reset passwords, deny access to unknown individuals and instructed how to block unwanted communications; students should be encouraged to invite known friends only and deny access to others
- Students should be advised not to publish specific and detailed private thoughts

How will filtering be managed?

- The college's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers
- The college will work with the Schools Broadband team to ensure that systems to protect students are reviewed and improved
- Norbury Manor will manage the configuration of its filtering; this task requires both educational and technical experience
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- The college's broadband access will include filtering appropriate to the age and maturity of students
- If staff or students discover unsuitable sites, the URL must be reported to the ICT Coordinator and/or the Network Manager
- Any material that the college believes is illegal must be reported to appropriate agencies such as the Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Command (CEOP Command)

How will videoconferencing be managed?

a) The equipment and network

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto-answer
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name
- External IP addresses should not be made available to other sites
- Videoconferencing contact information should not be put on the college website
- The equipment must be secure and if necessary locked away when not in use

- College videoconferencing equipment should not be taken off college premises without permission

b) Users

- Responsibility for the use of the videoconferencing equipment outside college time needs to be established with care
- Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure
- Parents and carers should agree for their children to take part in videoconferences, in the home/school agreement

c) Content

- Videoconferencing is a challenging activity with a wide range of learning benefits; preparation and evaluation are essential to the whole activity
- Videoconferencing should be supervised appropriately for students' ages
- Dialogue with other conference participants should be established before taking part in a videoconference; if it is a non-school site it is important to check that they are delivering material that is appropriate for your class
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights
- When recording a videoconference lesson, written permission should be given by all sites and participants; the reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference; recorded material shall be stored securely

How will emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in college is allowed
- Mobile phones will not be used during lessons or formal college time except for members of staff and sixth form students (out of lessons and in designated areas); the sending of abusive or inappropriate text messages is forbidden

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) - see separate Data Protection Policy and associated privacy notices

How will Internet access be authorised?

- The college will maintain a current record of all staff and students who are granted access to the college's electronic communications
- All staff and governors must read and sign the staff and governors acceptable use policy before using any college ICT resource

- Parents and students will be asked to sign and return a consent form for student access (possibly as part of the home/school agreement)
- Parents will be informed that students will be provided with supervised Internet access

How will risks be assessed?

- The college will take all reasonable precautions to ensure that users access only appropriate material; however, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a college computer; Norbury Manor cannot accept liability for the material accessed, or any consequences resulting from Internet use
- Methods to identify, assess and minimise risks will be reviewed regularly
- The college should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the college's complaints procedure
- Any issues (including sanctions) will be dealt with according to the college's disciplinary and child protection procedures
- All e-safety complaints and incidents will be recorded by the college including any actions taken
- Any complaint about staff misuse must be referred to the Headteacher
- Students and parents will be informed of the complaints procedure
- Parents and students will need to work in partnership with staff to resolve issues
- Discussions will be held with the local Police Safer Schools Partnership coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues

How is the Internet used across the community?

- The college will liaise with local organisations to establish a common approach to e-safety
- The college will be sensitive to Internet-related issues experienced by students out of college, e.g. social networking sites, and offer appropriate advice

How will cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in college; full details are set out in the college's policy on anti-bullying
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying; students, staff and parents/carers will be advised to keep a record of the bullying as evidence
- All incidents of cyberbullying reported to the college will be recorded
- There will be clear procedures in place to support anyone affected by cyberbullying

How will learning platforms (LPs) and learning environments be managed?

- Only members of the current student, staff and governor community will have access to the LP

- A visitor may be invited onto the LP by a member of the SLT; in this instance there may be an agreed focus or a limited time slot
- SLT and staff will monitor the usage of the LP by students and staff regularly in all areas, in particular message and communication tools and publishing facilities
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP
- Students may require editorial approval from a member of staff; this may be given to the student to fulfill a specific aim and may have a limited time frame

How will the policy be introduced to students?

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum; particular attention will be given where students are considered to be vulnerable
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use
- An e-safety module will be included in the PSHE, citizenship and/or ICT programmes covering both safe college use and safe home use
- e-safety rules will be posted in rooms with Internet access
- Student instruction in responsible and safe use should precede Internet access
- e-safety training will be part of the transition programme across the key stages and when moving between establishments
- All users will be informed that network and Internet use will be monitored

How will the policy be discussed with staff?

To protect all staff, governors and students, the college will implement acceptable use policies

- Staff training in safe and responsible Internet use both professionally and personally will be provided
- The e-safety policy will be formally provided to and discussed with all members of staff
- Staff should be aware that Internet traffic can be monitored and traced to the individual user; discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will be supervised by the senior leadership team and have clear procedures for reporting issues

How will parents' support be enlisted?

- Information and guidance for parents on e-safety will be made available to parents in a variety of formats
- A partnership approach with parents will be encouraged; this could include parents' evenings with demonstrations and suggestions for safe home Internet use or highlighting e-safety at other attended events ,e.g. parents' evenings, sports days
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents
- Parents' attention will be drawn to the college's e-safety policy in newsletters, the college brochure and on the college website
- Interested parents will be referred to relevant organisations

How will the college monitor the use of the Internet?

- Two programmes will be used to monitor all activity on the college network; Policy Central Enterprise allows us to track students who access material that breaches our acceptable use policies (AUPs) while LanSchool allows staff in the classroom to view the content of students' computer screens
- Breaches of either/both of these programs are referred to the DH and they will put into place the sanctions that follow
- Students not using the resource appropriately will be monitored and details recorded for future reference; copies of letters will be kept on file and screenshots sent home to parents
- Any issues that may involve child protection will also be referred to Chris Evans/Tracey Scarsbrook

What sanctions will be put in place for students who do not comply?

Category A infringements	Sanctions
• Use of non-educational sites during lessons including use of unauthorised instant messaging/social networking sites. (first offence)	• Loss of Internet access for a fixed period of time • Lunchtime or after college detention(s) • Head of year informed • Recorded on SIMS • Parents/carers informed
Category B infringements	**Sanctions**
• Continued use of non-educational sites during lessons after being warned • Continued use of unauthorised instant messaging/chatrooms, social networking sites, etc.	• Loss of Internet access rights for a more prolonged period of time • One day in seclusion • Head of year informed • Recorded on SIMS • Parents/carers informed
Category C infringements	**Sanctions**
• Deliberately corrupting or destroying someone's data • Violating the privacy of others or posting inappropriate messages, videos or images on a social networking site • Sending an email/tweet/message via any social media that is regarded as harassment or of a bullying nature (first offence) • Trying to access offensive material (including explicit music etc. [first offence])	• Loss of Internet access rights for a more prolonged period of time • Two days in seclusion • Head of year informed • Recorded on SIMS • Parents/carers informed
Category D infringements	**Sanctions**
• Continued sending of emails/tweets/messages via any social medium that is regarded as harassment, offensive or of a bullying nature after being warned • Deliberately creating, accessing, downloading or sharing any material deemed offensive, obscene, defamatory, racist, homophobic, extreme or violent • Sexting (sharing of inappropriate images either online or via mobile devices) • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 2018 • Bringing the college name into disrepute	• Loss of Internet access rights for a more prolonged period of time • Fixed-term exclusion • Recorded on SIMS • Head of year informed • Parents/carers informed • Evidence of infringement secured and preserved • Sender's email service provider informed • Liaison with the relevant service providers to facilitate removal of offending material • Report made to police/CEOP Command where necessary

An equality impact assessment has been carried out with regard to this policy. There was found to be no significant impact on any group with protected characteristics i.e. this policy does not discriminate against anyone on the basis of disability, gender re-assignment, pregnancy and maternity, race, religion or belief, gender or sexual orientation.

Appendix 1 - STUDENT INTERNET ACCEPTABLE USE AGREEMENT

All students must follow the conditions described in this policy when using college ICT networked resources including: Internet access, the college Learning Platform both in and outside of college.

Breaking these conditions will lead to:

- Withdrawal of the student's access
- Close monitoring of the student's network activity
- Investigation of the student's past network activity
- In some cases, criminal prosecution

Students will be provided with guidance by staff in the use of the resources available through the college's network. College staff will regularly monitor the network to make sure that it is being used responsibly.

The college will not be responsible for any loss of data as a result of the system or student mistakes in using the system. Students are advised to regularly back up their work.

CONDITIONS OF USE

Student access to the networked resources is a privilege - not a right. Students will be expected to use the resources for the educational purposes for which they are provided.

ACCEPTABLE USE

Students are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All use however should be consistent with the college ethos and code of conduct.

The following list does provide some examples that must be followed but this is not exhaustive:

1. I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the college into disrepute.

2. I will use appropriate language – I will remember that I am a representative of the college on a global public system; illegal activities of any kind are strictly forbidden.

3. I will not use language that could stir up hatred against any minority group; this includes creating, transmitting, displaying or publishing any material (text, images or sounds) that is likely to harass, cause offence, inconvenience or needless anxiety to any other person or group.

4. I am aware that I am responsible for my actions should I be found to be involved in Cyber-Bullying incidents both inside and outside of college hours; I will not undertake any activity that violates the privacy or dignity of myself or other users.

5. I am aware that I am morally and legally responsible for all that I write, publish and comment about on the internet (including social media platforms such as snapchat).

6. I realise that files held on the college network will be regularly checked by the Network Manager or other members of staff.

7. I will take responsibility for behaving safely and for all of my actions whilst using the internet; I will not attempt to visit websites that might be considered inappropriate or illegal; I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use; I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network and beyond.

8. I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to the Network Manager.

9. I understand that I am not allowed access to unsupervised and/or unauthorised chat rooms/social media sites and should not attempt to gain access to them.

10. I will not trespass into other users' files or folders; I will not share my login details (including passwords) with anyone else; likewise, I will never use other people's username and password; I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the Network Manager.

11. I will ensure that I log off after my network session has finished; if I find an unattended machine logged on under other usernames I will not continuing using the machine – I will log it off immediately.

12. I am aware that e-mail is not guaranteed to be private and any messages that fall short of the requirements of this policy will be followed up and dealt with appropriately.

13. I will not use the network in any way that would disrupt use of the network by others.

14. I will not download and/or install any unapproved software, system utilities or resources from the Internet.

15. I realise that students under <u>reasonable suspicion</u> of misuse in terms of time, activity or content <u>will</u> have their usage closely monitored or have their past use investigated.

16. I will not send or publish material that violates copyright law.

17. I will not attempt to harm or destroy any equipment, work of another user on the college network, or even another website or network connected to the college system.

18. I will not copy from the internet, other student's user area or shared areas and pass off subsequent work as my own; I understand that is plagiarism and is not acceptable to either the college nor to the exam boards in the case of coursework or controlled assessments.

19. I will not share my password with other students.

20. I understand that my internet use is closely monitored using forensic software and I am responsible for all internet use accessed using my log in details.

NETWORK SECURITY

If you discover a security problem, for example being able to access other users' data, you must inform the Network Manager immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

STUDENT DECLARATION:

- I accept the terms and conditions of the Norbury Manor Student ICT Acceptable Use Policy.

Signed: (student) Date:

PARENT/CARER DECLARATION:

- I have read the Norbury Manor Student ICT Acceptable Use Policy; I give my permission for my child to use the Norbury Manor ICT Network and Internet resources strictly under the terms and conditions outlined above
- I understand the full range of consequences should my child fail to comply with the above terms and conditions
- I understand that although Norbury Manor has implemented an Internet filtering service which aims to prevent access to inappropriate materials, this cannot always be guaranteed

Signed: (parent/carer) Date:

Appendix 2: Staff and Governors Internet Acceptable Use Policy

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

1. I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body
2. I will not reveal my password(s) to anyone
3. I will follow 'good practice' advice in the creation and use of my password; if my password is compromised, I will ensure I change it; I will not use anyone else's password if they reveal it to me and will advise them to change it
4. I will not allow unauthorised individuals to access email/Internet/intranet/network, or other school systems
5. I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols
6. I will not engage in any online activity that may compromise my professional responsibilities
7. I will only use the approved, secure email system(s) for any school business
8. I will only use the approved school email, school learning platform or other school approved communication systems with students or parents/carers and only communicate with them on appropriate school business
9. I will not browse, download or send material that could be considered offensive to colleagues
10. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager/school named contact
11. I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed
12. I will not publish or distribute work that is protected by copyright without first checking the relevant permissions
13. I will not connect a computer, laptop or other device (including USB flash drive) to the network/Internet that does not have up-to-date anti-virus software and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems
14. I will not use personal digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home without permission
15. I will use the school's learning platform in accordance with school protocols
16. I will ensure that any private social networking sites/blogs etc that I create or actively contribute to are not confused with my professional role
17. I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs
18. I will access school resources remotely (such as from home) only through the LGfL/school approved methods and follow e-security protocols to access and interact with those materials

19. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location
20. I understand that data protection policy requires that any information seen by me with regard to staff or student information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority
21. I will embed the school's e-safety curriculum into my teaching
22. I will alert the school's named child protection officer/relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern
23. I will only use LA systems in accordance with any corporate policies
24. I understand that all Internet usage/and network usage can be logged and this information could be made available to my manager on request
25. I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or students) which I believe may be inappropriate or concerning in any way, to a senior member of staff/named child protection officer at the school
26. I understand that failure to comply with this agreement could lead to disciplinary action
27. I will not add current Norbury Manor students or recent leavers to personal social networking sites
28. I will adhere to the college's GDPR Policy
29. I will report immediately any data breaches to the college's Data Protection Officer (DPO)

User Signature

- I agree to abide by all the points above
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies
- I wish to have an email account; be connected to the Intranet and Internet; and be able to use the school's ICT resources and systems

Signature Date

Full name (printed)

Job title

School

Appendix 3: Norbury Manor Staff and Governors Laptop Agreement and Tax Declaration

<DATE>

Name | **Laptop Asset Number** 00____

I understand that my use of a college laptop is strictly under the following terms and conditions:

- The laptop is my sole responsibility
- I may take the laptop home for college use; should I allow it to be used by any third party, I understand I will be responsible for any resulting damage or loss that may occur and also any tax implications that arise from my personal use of the laptop (see below)
- When not in use at home I will ensure that it is out of sight
- I must not leave it unattended at any time unless it is in a locked office
- I understand that I may not download any software to the laptop without specific authorisation from Patrick Harris (Network Manager)
- I understand that I may not set up an Internet connection for simultaneous home and college use
- I understand that I must report any damage or faults with the laptop as soon as they emerge to Patrick Harris (Network Manager)
- I understand that the college's acceptable Internet use policy also applies to the laptop
- The laptop must be returned to Norbury Manor upon the completion of my contract of employment at the college or the end of my period of office as a governor
- I declare that any computer equipment provided by the college for my use at home during the tax year **<DATE>** has been and will be used only for college purposes, and that any private use will be insignificant and incidental
- I will observe the requirements of the GDPR as they apply to the use and access of staff or student data at Norbury Manor

The college will exercise its right to monitor the use of the college's laptops, including the monitoring of websites, the interception of emails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the laptop is or may be taking place, or the laptop is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Signed:

Date:

Appendix 4: What is E-safety?

Norbury Manor's e-safety policy reflects the importance it places on the safe use of information systems and electronic communications.

E-safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- E-safety concerns safeguarding children and young people in the digital world
- E-safety emphasises learning to understand and use new technologies in a positive way
- E-safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online
- E-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of college

Some of the material on the Internet is published for an adult audience and can include violent and adult content. Information on weapons, crime and racism may also be unsuitable for children and young people to access. Students need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Colleges have a duty of care to enable students to use on-line systems safely.

The college needs to protect itself from legal challenge and ensure that staff, visitors and governors work within the boundaries of professional behaviour. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use email, text or instant messaging (IM) to 'groom' children.

The college can help protect itself by making it clear to students, staff, governors and visitors through the acceptable use policies that the use of college equipment for inappropriate reasons is "unauthorised."

E-safety training should be an essential element of staff induction and part of an ongoing CPD programme. However, the college should be aware that a disclaimer is not sufficient to protect it from a claim of personal injury and therefore we need to ensure that all reasonable actions have been taken and measures put in place to protect users.

The rapid development and accessibility of the Internet and new technologies such as personal publishing and social networking means that e-safety is an ever growing and changing area of interest and concern. The college's e-safety policy must reflect this by keeping abreast of the vast changes taking place around us.

The college's e-safety policy must operate in conjunction with other college policies including those relating to behaviour, child protection and anti-bullying. E-safety must be built into the curriculum.

Appendix 5: Notes on the Legal Framework

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18.

Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise).

This can include images taken by and distributed by the child themselves (often referred to as “sexting”). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust (typically, teachers, social workers, health professionals, connexions staff, etc. fall into this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Colleges should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 2018

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual.

The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1-3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- Gain access to computer files or software without permission (for example using someone else's password to access files)
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

This can include racist, xenophobic and homophobic comments, messages, etc.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form.

Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17-29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to college activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Under Section 63 it is an offence to possess an “extreme pornographic image”.
Section 63 (6) states the image must be “grossly offensive, disgusting or otherwise obscene”. As per section 63 (7) this includes “explicit and realistic” images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead”.

Penalties can be up to three years' imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for colleges which relate to cyberbullying/bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of students off-site

- College staff are able to confiscate items such as mobile phones, etc. when they are being used to cause a disturbance in class or otherwise contravene the college behaviour/anti-bullying policy

Appendix 6: Use of Social Media Tools as a College

Social media tools, such as blogs, wikis, social networking sites and video sharing sites (e.g. Twitter, YouTube, Facebook, etc.) can be fantastic for teaching and learning. These tools can also help to engage with parents/carers and the wider community. However, it is essential that their use is carefully considered by us as a college.

Good e-safety practice must be fully embedded across the establishment (such as whole-staff e-safety training, social media 'training' for staff and students and parental awareness inputs) before colleges can consider using social media tools.

The decision on using social media tools must be made as a college and should only take place with full support and backing by the senior leadership team (SLT). The use of social media tools must be fully documented and risk assessed and outlined in the e-safety policy. The college will need to be aware of their responsibility regarding moderating any content and to ensure that the service is kept up to date. The tools must also be used in accordance with the college's behaviour and complaints policies.

Firstly, it is essential that the correct tool is selected; for example, when communicating with parents and carers about college-based decisions it might be better to use a blog to enable a discussion rather than a Twitter page. Colleges should also – where possible – use tools available on their college website or learning platform.

Crucial to selecting the appropriate social media tool is deciding who the target audience is (parents/carers or students, etc.). Colleges will need to be aware that not all families will have access to technology at home. To combat this issue some colleges have offered open evenings to families or have an Internet-enabled computer in an accessible location for parents/carers to access after signing an acceptable use policy. It is also important to find out if your audience would like to engage with the college via such media, for example some students may not wish to add their college on a social networking site.

It is important that colleges are aware how social media sites function and are aware how to make them as safe as possible, such as making profiles "private" or using groups to engage with the community instead of profiles.

When using social media with children, colleges must be aware of site age restrictions and only use sites that are deemed to be age appropriate and suitable for educational purposes.

Such tools will also need to be moderated and regulated frequently as very few social media tools are able to verify and authenticate users appropriately, unless the system is controlled directly by the college or by a subscription service.

Where possible when using services which the college cannot control (e.g. Facebook, Twitter, YouTube) then it is recommended that comments etc. are approved before they are made live and membership to online groups etc. is controlled (e.g. people must request to join a group or follow).

In order to protect staff, professional accounts, pages or profiles must be used when communicating with students or the college community. College approved email addresses and contact details should be used and staff should not share any personal contact details or information with students or parents/carers.

Appendix 7: What do we do if…

An inappropriate website is accessed <u>unintentionally</u> in college by a teacher or child?

1. Play the situation down; don't make it into a drama.
2. Report to the head of year/e-safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the Network Manager and ensure the site is filtered (LGfL schools report to: **webalerts@synetrix.com**).
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> by a child?

1. Report to the head of year/e-safety officer.
2. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
3. Notify the parents of the child.
4. Inform the Network Manager and ensure the site is filtered if need be.
5. Inform the LA if the filtering service is provided via an LA/RBC.

An adult uses college ICT equipment inappropriately?

1. Report the misuse immediately to the Headteacher/e-safety officer who will ensure that there is no further access to the PC or laptop.
2. If the material is offensive but not illegal, the Headteacher/e-safety officer should:
   - Remove the PC to a secure place
   - Instigate an audit of all ICT equipment by the colleges ICT managed service providers to ensure there is no risk of students accessing inappropriate materials in the college
   - Identify the precise details of the material
   - Take appropriate disciplinary action (contact Human Resources)
   - Inform governors of the incident
3. In an extreme case where the material is of an illegal nature:
   - Contact the local police or Hi-Tech Crime Unit and follow their advice
   - If requested, remove the PC to a secure place and document what you have done

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of college time?

1. Inform the head of year/e-safety officer who will:
   - Advise the child not to respond to the message
   - Refer to relevant policies including e-safety, anti-bullying and PSHE and apply appropriate sanctions
   - Secure and preserve any evidence
   - Inform the sender's email service provider
   - Notify parents of the children involved
   - Inform the police if necessary

licious or threatening comments are posted on an Internet site about a student or member of staff?

1. Inform Headteacher/e-safety officer who will:

- Secure and preserve any evidence
- Inform and request the comments be removed if the site is administered externally
- Send all the evidence to CEOP Command at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child?

1. Report to the named Child Protection Officer/e-safety officer in college who will:
   - Advise the child on how to terminate the communication and save all evidence
   - Contact CEOP Command at http://www.ceop.gov.uk/
   - Consider the involvement of police and social services

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the Internet or mobile technology; they must be able to do this without fear.

Appendix 8: E-safety Contacts, Resources and References

- CEOP Command www.ceop.police.uk
- Childline www.childline.org.uk
- Childnet International www.childnet.com
- Click Clever Click Safe http://clickcleverclicksafe.direct.gov.uk
- Cybermentors www.cybermentors.org.uk
- Digizen www.digizen.org.uk
- Internet Watch Foundation (IWF) www.iwf.org.uk
- Kidsmart www.kidsmart.org.uk
- London Grid for Learning www.lgfl.net
- Parenting in the Digital Age (PitDA) www.pitda.c.uk
- Teach Today http://en.teachtoday.eu
- Think U Know website www.thinkuknow.co.uk
- Virtual Global Taskforce — Report Abuse www.virtualglobaltaskforce.com
- Webwise www.bbc.co.uk/webwise

Further sources of information

<u>Government guidance and support</u>

- *Relationship Education, Relationships and Sex Education and Health Education* - statutory guidance
- *National curriculum in England: computing programmes of study* - statutory guidance on computing programmes of study
- *National curriculum in England: citizenship programmes of study* – statutory programmes of study and attainment targets for citizenship at key stages 3 and 4
- *Keeping Children Safe in Education* - statutory guidance for schools and colleges on safeguarding children and safer recruitment
- *Behaviour and discipline in schools* - guidance for school leaders and staff on developing a school behaviour policy, and a checklist of actions to take to encourage good behaviour

- *Searching, screening and confiscation at school* - guidance explaining the powers schools have to screen and search students, and to confiscate items they find

- *Thinkuknow Programme* - *o*nline safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation; education resources and online advice for children aged 4–18, expert support and professional development for the children's workforce; signposts to the National Crime Agency's Click CEOP service for children to report concerns related to sexual abuse

- *National Centre for Computing Education (NCCE)* - this has been set up to support the teaching of computing education throughout schools and colleges in England, giving teachers the subject knowledge and skills to establish computing as a core part of the curriculum and to help primary and secondary schools teach the safety and security aspects of the National Curriculum Computing Programme of Study, the National Centre for Computing Education's resource repository and professional development courses covering objectives from the Education for a Connected World framework; the resource repository's lesson plans will include links to the framework, as well as specific activities for non-specialist teachers

- *UK Council for Internet Safety* - the UK Council for Internet Safety expands the scope of the UK Council for Child Internet Safety to achieve a safer online experience for all users, particularly groups who suffer disproportionate harms; the website has useful resources for schools and parents to help keep children safe online including Education for a Connected World – a framework which describes the digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives; it highlights what a child should know in terms of current online technology, the influence on behaviour and development of online technology, and what skills children need to be able to navigate it

- *UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use* - published February 2019

<u>For parents and carers</u>

- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world; their support for parents includes a range of downloadable guides covering subjects such as transition to secondary school, vlogging and livestreaming, online gaming and cyberbullying

- NSPCC - offers a range of resources to help parents keep children safe when they're using the Internet, social networks, apps, games and more

- Parent Info - from CEOP Command and Parent Zone, Parent Info is a website for parents covering all of the issues amplified by the Internet; it is a free service which helps schools engage parents with expert safety advice, endorsed by the National Crime Agency's CEOP Command; this website provides expert information about a range of online harms

- Parent Zone - offers a range of resources for families, to help them meet the challenges of the digital age, including parent guides on the latest digital trends and platforms

For students

- BBC Own It – support for young people to take control of their online life, including help and advice, skills and inspiration on topics such as friendships and bullying, safety and self-esteem

- Childline – includes information for students on sexting, gaming, grooming, bullying, porn, relationships

National organisations for schools

- The Anti-bullying Alliance - a coalition of organisations and individuals, working together to stop bullying and create safer environments in which children and young people can live, grow, play and learn; their website includes a range of tools and resources to support schools in preventing and tackling cyberbullying

- Childnet - a children's charity whch has a wide range of practical resources freely available covering all online safety issues that are available for teachers working with children of all ages, including those with special educational needs (SEN)

- The Diana Award – a charity running a number of different projects aimed at reducing bullying in schools; their resource section has information to help schools tackle cyberbullying along with resources from their Be Strong Online Ambassador programme – a peer-led initiative which aims to empower young people to increase the digital resilience of their peers

- DotCom Digital - a free resource for schools, created by children with Essex Police and the National Police Chief Council Lead for Internet Intelligence and Investigations; the resource aims to prevent young people becoming victims of online grooming, radicalisation, exploitation and bullying by giving them the confidence to recognise warning signs and reach out to an adult for help

- The Hopes and Streams report by LGfL has themed chapters that include links to online resources and ideas for tackling the issues raised

- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world, they also have a dedicated section of their website for professionals which includes resources to support staff training, whole school programmes and policies and a parent pack to help schools engage with parents about online safety

- Internet Watch Foundation – an Internet hotline for the public and IT professionals to report potentially criminal online content, including child sexual abuse images

- Parent Zone's dedicated school zone - includes a range of resources to support teachers educate their students on how to stay safe online, what to do if they find themselves in an uncomfortable situation and how to build their digital resilience

- PSHE Association - the national body for Personal, Social, Health and Economic (PSHE) education; their programme of study for PSHE education aims to develop skills and attributes such as resilience, self-esteem, risk-management, team working and critical thinking; they also have many guides about how to teach specific topics

- SWGfL – a charity dedicated to empowering the safe and secure use of technology; their website includes a range of free resources for schools covering a range of online safety issues, including digital literacy/critical thinking and consequences of sharing and publishing images

- UK Safer Internet Centre –a partnership between Childnet International, Internet Watch Foundation and SWGfL to promote the safe and responsible use of technology for young people; their website includes a range of practical resources and support for schools including 360 degree safe - a free-to-use self-review tool for schools to assess their wider online safety policy and practice

- A Helpline – this helpline was established to support those working with children across the UK with online safety issues; operated by SWGfL, it can be contacted on 0344 381 4772 and via helpline@saferinternet.org.uk

- Safer Internet Day - the UK Safer Internet Centre organises Safer Internet Day for the UK and each year develops a range of materials from assemblies to lesson plans, posters to quizzes for each key stage to address a key online safety issue

Appendix 9: E-safety Infringement Letter

DATE

Dear Parents and/or Carers,

Re:

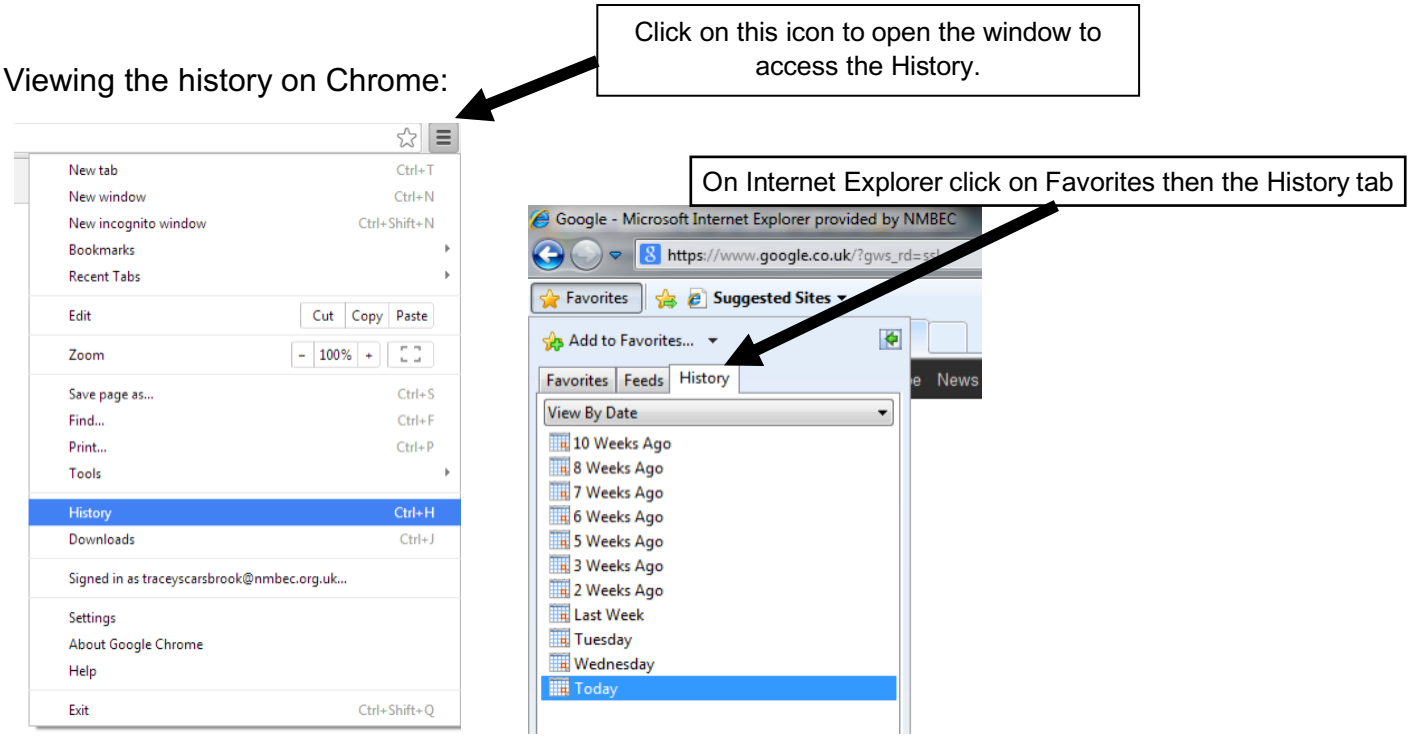
I am writing to inform you that during our regular monitoring of the use of the Internet at Norbury Manor it has come to light that your child has broken the college Internet Acceptable Use Policy.

On this occasion your child has:

As a result she will:

We would also advise you to review your child's Internet use at home in order to ensure that this type of activity is not also happening there. You can do this by viewing the "history" on your child's laptop, PC or other device.

Viewing the history on Chrome:



How will this infringement be handled?

We take our commitment to e-safety seriously and whenever a student infringes our e-safety policy, the final decision on the level of sanction will be at the discretion of the college management and will reflect the college's behaviour and disciplinary procedures.

As a guide the sanctions would escalate as below:

Category A infringements	**Sanctions:**
● Use of non-educational sites during lessons including use of unauthorised instant messaging/social networking sites (first offence)	● Loss of Internet access for a fixed period of time ● Lunchtime or after college detention(s) ● Head of year informed ● Recorded on SIMS ● Parents/carers informed
Category B infringements	**Sanctions:**
● Continued use of non-educational sites during lessons after being warned ● Continued use of unauthorised instant messaging/chatrooms, social networking sites, etc.	● Loss of Internet access rights for a more prolonged period of time ● 1 day in seclusion ● Head of year informed ● Recorded on SIMS ● Parents/carers informed
Category C infringements	**Sanctions:**
● Deliberately corrupting or destroying someone's data ● Violating the privacy of others or posting inappropriate messages, videos or images on a social networking site ● Sending an email/tweet/message via any social media that is regarded as harassment or of a bullying nature (first offence) ● Trying to access offensive material (including explicit music etc. [first offence])	● Loss of Internet access rights for a more prolonged period of time ● 2 days in seclusion ● Head of year informed ● Recorded on SIMS ● Parents/carers informed
Category D infringements	**Sanctions:**
● Continued sending of emails/tweets/messages via any social media that is regarded as harassment, offensive or of a bullying nature after being warned ● Deliberately creating, accessing, downloading or sharing any material deemed offensive, obscene, defamatory, racist, homophobic, extreme or violent ● Sexting (sharing of inappropriate images either online or via mobile devices) ● Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 2018 ● Bringing the college's name into disrepute	● Loss of Internet access rights for a more prolonged period of time ● Fixed term exclusion ● Recorded on SIMS ● Head of year informed ● Parents/carers informed ● Evidence of infringement secured and preserved sender's email service provider informed ● Liaison with the relevant service providers to facilitate removal of offending material ● Report made to police/CEOP where necessary

We will continue to monitor your child's Internet use once access is returned and if similar infringements occur we will be forced to escalate the sanctions as they appear above. We hope that

this proves to be an isolated incident and that your daughter will learn that her actions whilst using the Internet have consequences that are far reaching and can potentially be very serious.

Thank you for your continuing support and please do contact us if you require any further information or clarification of anything contained in this letter.

My email address is: traceyscarsbrook@nmbec.org.uk and my telephone number is 020 8679 0062 ext. 240.

Yours sincerely,

Tracey Scarsbrook

Deputy Headteacher

Appendix 10 - Teaching About Online Safety - Underpinning Knowledge and Behaviour

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up-to-date with the latest devices, platforms, apps, trends and related threats.

It is therefore important to focus on the underpinning knowledge and behaviours that can help students to navigate the online world safely and confidently regardless of the device, platform or app. This teaching could be built into existing lessons across the curriculum, covered within specific online safety lessons and/or school-wide approaches. Teaching must always be age- and developmentally appropriate.

Underpinning knowledge and behaviours include:

How to evaluate what they see online

This will enable students to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable. Schools can help students consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information?
- What's behind this post?
- Is this too good to be true?
- Is this fact or opinion?

How to recognise techniques used for persuasion

This will enable students to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity. Schools can help students to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation)
- Techniques that companies use to persuade people to buy something, ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- Criminal activities such as grooming

Online behaviour

This will enable students to understand what acceptable and unacceptable online behaviour look like. Schools should teach students that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach students to recognise

unacceptable behaviour in others. Schools can help students to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online, for example, how anonymity ("you do not know me") and invisibility ("you cannot see me") affect what people do
- Looking at how online emotions can be intensified, resulting in mob mentality
- Teaching techniques (relevant online and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online
- Considering unacceptable online behaviours often passed off as so-called social norms or "just banter"; for example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline

How to identify online risks

This will enable students to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help students assess a situation, think through the consequences of acting in different ways and decide on the best course of action. Schools can help students to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online
- Discussing risks posed by another person's online behaviour
- Discussing when risk taking can be positive and negative
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint; this could include longer-term considerations, i.e. how past online behaviours could impact on students' futures., e.g. when applying for a place at university or a job
- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

How and when to seek support

This will enable students to understand safe ways in which to seek support if they are concerned or upset by something they have seen online. Schools can help students by:

- Helping them to identify who trusted adults are
- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and third sector organisations such as Childline and Internet Watch Foundation; this should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education)
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported

Vulnerable students

Any student can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance; however, there are some students - for example, looked after children and those with special educational needs - who may be more susceptible to online harm or have less support from family or friends in staying safe online. Schools should

consider how they tailor their offer to ensure these students receive the information and support they need.

The following resources can help schools consider how best to support their most vulnerable students in staying safe online:

- Vulnerable Children in a Digital World - Internet Matters
- Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group section
- STAR SEN Toolkit – Childnet

Teaching about online harms and risks in a safe way

As with any safeguarding lessons or activities, it is important that schools consider the topic they are covering and the potential that a child (or more than one child) in the class may be suffering from online abuse or harm in this way.

It is important to create a safe environment in which students feel comfortable to say what they feel. If a student thinks they will get into trouble and/or be judged for talking about something which happened to them online they may be put off reporting it and getting help.

Where schools are already aware of a child who is being abused or harmed online they should carefully plan any lesson to consider this, including not drawing attention to that child in a way that would highlight or publicise the abuse. It is good practice to include the designated safeguarding lead (or a deputy) when considering and planning any safeguarding related lessons or activities (including online) as they will be best placed to reflect and advise on any known safeguarding cases, and how to support any students who may be especially impacted by a lesson.

In some cases, a student will want to make a disclosure following a lesson or activity. The lesson may have provided the knowledge that enabled the students to realise they are being abused or harmed and/or give them the confidence to say something. This is why it is essential all students are clear what the school's reporting mechanisms are. As per "Keeping Children Safe in Education" those mechanisms should be child friendly and operate with the best interests of the student at their heart.