Norbury Manor Business & Enterprise College *for* Girls

ICT Policy

Review date: **June 2018**

Next review date: **June 2019**

Staff resp. for review: **TS**

Realising potential, nurturing leaders of the future

Cross Curricular ICT Policy

To be read in conjunction with the more detailed E-safety Policy and also the attached appendices:

- Appendix 1: Student Acceptable Use Policy
- Appendix 2: Staff and Governors Acceptable Use Policy
- Appendix 3: Staff Laptop Agreement

Hardware Resources
Norbury Manor has a whole college network split into a curriculum network and an administrative network. Most subject areas have access to their own ICT facilities in addition to the 7 dedicated ICT/business studies suites and the Sixth Form Study Room and breakout spaces.

The college also has additional hardware such as portable data projectors, scanners, printers, video conferencing equipment, IRIS Connect and digital still and video cameras available on a bookable basis for staff and students to use.

We have also invested in the purchase and utilisation of interactive whiteboard technology. All classrooms and many public areas have access to interactive whiteboards and data projectors to enhance teaching and learning.

The college has an established wireless network operating across the whole college site.

We also operate an extensive administration network running the SIMS.net suite of programmes which operates the college MIS system. The MIS system can also be accessed via the curriculum network.

Software Resources
Departments are responsible for ensuring that any software purchased for their department are compatible with the network and that they are installed by the Network Manager. The Network Manager is responsible for ensuring that any software installed by him complies with the relevant licensing agreements.

Software can be ordered via the Network Manager who will trial programmes and report to HoDs on the compatibility of the software.

New Purchases
Any department wishing to increase the numbers of computers or peripherals in their areas should consult the Network Manager and make representation to TS in a bid format and as many requests as possible will be included in the ICT Development Plan for the coming year.

Ordering of Stock
Printer cartridges etc for the ICT rooms are ordered centrally by the Network Manager who shops around for the best deal at the time. Colour cartridges are entirely the responsibility of the department who “own” the colour printer.

In addition to this, departments who use headphones and other similar items are responsible for their care and maintenance and also the cost of replacement.

IWB pens and remote controls come as standard with the IWB packages we buy, but if they are lost they are the responsibility of the individual departments to replace.

Preventing Wastage
Students should be aware of the need to avoid waste. Practices such as excessive use of the colour printer, use of excessively large, inappropriate fonts, making hard copies of whole articles from the Internet should be discouraged by all staff.

All used paper should be recycled via the boxes provided. The college operates a 'Think Before You Print' policy.

Maintenance
The Network Manager is responsible for the day to day running of the computers, including taking back-ups. He is supported by a full time Assistant Network Manager and 1 ICT technician.

For more serious problems he will contact the RM hotline and the CAPITA help line with whom we have service contracts.

Staff and Students' Use of the College Network
Student and staff use of the college network is monitored by the Deputy Headteacher. Students and their parents are required to sign the Acceptable Use Policy (Appendix 1). Students' accounts are monitored regularly by the Deputy Headteacher and access will be removed if students are found to be disobeying the conditions outlined in the Acceptable Use Policy.

All students in the college are inducted in the CEOPS programme on internet safety. Incidents of students placing themselves at risk through their unsafe use of the internet are followed up by the Deputy Headteacher and sanctions can be issued including loss of internet privileges etc. Parents will also be informed.

All staff are informed annually of the college's Acceptable Use Policy (Appendix 2). All staff are also required to sign a laptop policy pro forma in order to accept responsibility for their laptops (Appendix 3). Staff accounts are also monitored on a regular basis.

When using ICT in a lesson, staff are required to make use of the LanSchool programme in order to monitor students appropriate use of ICT in the lesson to prevent them being off-task.

E-safety (refer to full E-safety Policy)
As E-safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. The school has a framework for teaching internet skills in ICT/ PSHE lessons.

Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

New staff receive information on the school's acceptable use policy as part of their induction. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community. All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas. eSafety posters will be prominently displayed.

INSET

Teachers are encouraged to attend in-house CPD relating to ICT in their subject areas or in the use of the MIS System. The ICT department will provide INSET at the request of any department by arrangement after college.

GDPR and Data Protection
All staff and students are expected to abide by the college's data protection policy, guided by the requirements of the Data Protection Act 2018 and General Data Protection Regulation (GDPR), when using the college's ICT network.

In particular, staff should be careful of using their laptops in public areas of the college where student data could be on display wirelessly from the MIS system. Similarly, when using the MIS system in the classroom on a public PC it is essential that the PC is not left open with student/staff data being displayed.

Staff have been issued with encrypted memory sticks to hold confidential data while we transition this year to a cloud-based system of storage.

Staff also need to ensure that any data relating to students and stored on their laptops is not accessed by their family members at home when the laptop is being used offsite.

This policy needs to be read in conjunction with:

- The Behaviour and Anti-Bullying Policy
- The E-safety Policy
- The Child Protection Policy

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.

Updated June 2018

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 Twitter, Facebook, etc.).

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 **reasonable suspicion** of misuse in terms of time, activity or content **will** have their usage closely monitored or have their past use investigated.

16. I will not receive, 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.**

- 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
- I will not reveal my password(s) to anyone
- 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
- I will not allow unauthorised individuals to access email/Internet/intranet/network, or other school systems
- 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
- I will not engage in any online activity that may compromise my professional responsibilities
- I will only use the approved, secure email system(s) for any school business
- 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
- I will not browse, download or send material that could be considered offensive to colleagues
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager/school named contact
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed
- I will not publish or distribute work that is protected by copyright
- 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
- 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
- I will use the school's learning platform in accordance with school protocols
- 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
- 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

- 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
- 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
- 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
- I will embed the school's e-safety curriculum into my teaching
- 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
- I will only use LA systems in accordance with any corporate policies
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request
- 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
- I understand that failure to comply with this agreement could lead to disciplinary action
- I will not add current Norbury Manor students or recent leavers to personal social networking sites
- I will adhere to the college's GDPR Policy
- 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 & Tax Declaration

<DATE>

Name | **Laptop Asset Number** 0 0 _ _ _ _

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 (college Network Manager)
- I understand that I may not set up an internet connection for simultaneous home and school use
- I understand that I must report any damage or faults with the laptop as soon as they emerge to Patrick Harris (college 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 it applies 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:**