Procedure on Responsible Behaviour in Cyber Space

THIS POLICY INCLUDES THE EARLY YEARS FOUNDATION STAGE [EYFS]

NOTTINGHAM HIGH SCHOOL

Procedure on Responsible Behaviour in Cyber Space

Contents

Procedure on Responsible Behaviour in Cyber Space

Introduction

Nottingham High School is aware that students often have access to technologies that have both positive and negative potential. Online safety is part of the School's wider safeguarding strategy and the latest version of the School's Safeguarding and Child Protection policy can be found at:

https://nottinghamhigh.co.uk/policies

This Procedure is concerned with students' responsible behaviour in cyber space. See also the NHS ICT 'Acceptable Use' policies, found at the above website.

Clear guidance is given to staff and pupils on acceptable use of technology in the School's various relevant policies and procedures. Visitors to the School have access, via a regularly altered code, to a separate network which has its own filtering system. At the point access is granted to the network, information is given about appropriate use.

Abbreviations used in this document: NHS = Nottingham High School, DSL = Designated Senior Lead. PSHE = Personal, Social, Health and Economic Education, ICT = Information and Communications Technology

1. The Role of ICT in Our Students' Lives

We fully accept that ICT plays an enormously important part in the lives of all young people. Outside school sophisticated games consoles, together with Bluetooth, mobile internet and Wi-Fi-enabled devices, provide unlimited access to the internet, to SMS messages, to blogging services, social media platforms, to Skype, to wikis, chat rooms, social networking sites and video sharing sites.

The continued communications revolution gives young people unrivalled opportunities. It also brings risks. We see that an important part of our role at NHS is, through ICT lessons, PSHE lessons and assemblies, to educate our students in how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, harassment, grooming, sexting, stalking and abuse, child sexual exploitation, female genital mutilation, so-called honour-based abuse, forced marriage, cyberbullying, and mental health. They also need to learn how to be resilient in the online environment and to avoid the risk of exposing themselves to subsequent embarrassment, hence 'over blocking' is not normal practice. Protecting our students through education and information is paramount.

Students are taught in lessons, through assemblies and PSHE about online safety, appropriate use of social media and how to research on the internet and to evaluate sources. They are educated in the importance of evaluating the intellectual integrity of different websites, and why some apparently authoritative sites need to be treated with caution. Some sites, for example, that are racist,

homophobic, jihadist etc. masquerade as being serious, historical or impartial. Some free online encyclopaedias do not evaluate or screen the material posted on them.

The Internet and online world provides access to a wide-range of content, some of which is harmful and has become a significant component of many safeguarding issues. Extremists, CSE and sexual predation are all facilitated by the internet and can lead to harm. As a School we place highly the importance of online safety for our students. The filtering and monitoring system used in our school blocks inappropriate content whilst allowing the students a safe environment to learn. We currently filter social media sites to ensure age-appropriate access to students.

Although students have unfiltered internet access when using their mobile phone or other personal device, this procedure still applies to the use of those devices in school. As a School we acknowledge the importance of monitoring students with mobile data access to networks and will be alert to students using this type of network access whenever possible. Staff have an awareness of the need to do this. In order to ensure the security of the computer network and the health and safety of students, the School will exercise its right by electronic means to monitor the use of the computer systems and network. This includes, but is not limited to, the monitoring of:

- web sites visited,
- printer usage,
- interception of email,
- the deletion of inappropriate materials, and
- the storing of text, imagery or multimedia files which are unauthorised or unlawful.

2. Role of NHS ICT Staff

With the explosion in computing technology, we recognise the need for improved filters that are continually under review. However, we must also balance this with the need to give our students responsible and safe access to the internet. Our ICT staff have a key role in maintaining a safe technical infrastructure at the School and to keep abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of ICT.

Our ICT staff use the Smoothwall system, including their email notifications, for up-to-date information which reflects current trends, and this is cascaded to the DSL and other staff when appropriate. Searches and web addresses are monitored and the ICT technicians will alert the DSL and senior staff where there are concerns and prevent further access when new sites that are unblocked are found. The ICT department understand that they must inform the DSL immediately of any safeguarding concerns that occur through their regular checks. Other breaches displaying inappropriate use of ICT by students or staff must be passed on to SMT. The Smoothwall system emails members of the Senior Management Team and the IT Manager when individual students attempt to access filtered material.

Our ICT staff regularly discuss online safety issues, including around SPAM, and plan responses accordingly.

3. Role of Our Designated Senior Lead

We recognise that online safety is a child protection and general safeguarding issue.

The DSLs and DDSLs are conversant with the safety issues involved with the misuse of the internet and other mobile electronic devices. They update staff annually on current online safety matters and reiterate the importance that staff play in protecting and educating students online. They work closely with NHS ICT staff and the Local Safeguarding Children's Board (LSCB) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of NHS. The DSL has regular conversations with the ICT staff, checking the filter systems on the School network to ensure the students in the school are not at risk.

We aim to teach all of our students to understand why they need to behave responsibly if they are to protect themselves.

4. Role of Staff

There is a clear reporting mechanism for staff to highlight any concerns. The IT Helpdesk email address is monitored by the ICT Department who will react quickly to any issues raised. Staff are trained by the DSL to use an online safeguarding form, or telephone or email if required, when they have any safeguarding concerns raised by online behaviour.

5. Responsible Use of the Internet and Electronic Devices at NHS

"Children and young people need to be empowered to keep themselves safe. This isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool, we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim." Dr Tanya Byron "Safer Children in a digital world: the report of the Byron Review".

Our guiding principles are:

Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our School's Anti-Bullying Policy describes our preventative measures and the procedures that will be followed when we discover cases of bullying, including bullying of those with protected characteristics.

- Peer-on-peer cyberbullying is also recognised as a potential safeguarding concern. Staff are trained to be alert to this which may particularly display itself as sexting. See further advice below.
- Proper supervision of students plays an important part in creating a safe ICT environment at school; but everyone needs to learn how to stay safe outside the School.

Sexting:

- The sending of an indecent image can be illegal. A person under-18 is committing an offence if they send an indecent image of themselves. Someone passing this on is also distributing an indecent image of a child. The School seeks to protect children from sexting and the significant impact it can have. Advice for students is available at:
  www.thinkuknow.co.uk
  https://www.childline.org.uk/explore/onlinesafety/pages/sexting.aspx

  Advice for parents is available at:
  https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Treating other ICT users with respect

- We expect students to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always meet the School's expectations.
- We expect a degree of formality in communications between staff and students and would not normally expect them to communicate with each other by text or mobile phones. Our Off-Site Visits policy explains the circumstances when communication by mobile phone may be appropriate. In such circumstances, staff use School, as opposed to personal, mobiles and students' mobile numbers are deleted at the end of the visit. Students are also instructed to delete staff numbers.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Our Anti-Bullying Policy is on our website.
- Sanctions will be issued for misuse of devices, bullying and use of inappropriate sites or material as per the School's Behaviour and Discipline policy and Anti Bullying policy.
- All students are encouraged to look after each other and to report any concerns regarding the misuse of technology, or worrying issue to their tutor or another member of staff.

Procedure on Responsible Behaviour in Cyber Space

Keeping the School Network Safe

- Certain sites are blocked by our filtering system and our ICT Department monitors students' use of the network.
- The ICT Department monitors email traffic and blocks SPAM and certain attachments.
- We issue all students with their own personal school email address. Access is via personal login, which is password protected. We give guidance on the reasons for always logging off and for keeping all passwords securely.
- We have strong anti-virus protection on our network, which is operated and continually reviewed by the ICT Department.

Promoting Safe Use of Technology

Students of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- www.thinkuknow.co.uk
- www.saferinternet.org.uk
- www.internetmatters.org
- www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
- Cyberbullying (www.cyberbullying.org)
- Bullying UK (www.bullying.co.uk)

As mentioned previously, ICT assemblies and PSHE lessons cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. Guidance covers topics such as saving yourself from future embarrassment, explaining that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.

Safe Use of Personal Electronic Equipment

- Our guidance is that no one should put anything onto the web that they would not say to a parent.
- We offer guidance on the safe use of social networking sites and cyberbullying in PSHE lessons.
- Our PSHE lessons include guidance on how students can identify the signs of a cyber-stalker, and what they should do if they are worried about being harassed or stalked online.
- We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.

Procedure on Responsible Behaviour in Cyber Space

Considerate Use of Electronic Equipment

- Staff may confiscate personal equipment that is being used inappropriately during the school day. Such items may be retained by staff at the direction of the Deputy Head (Individuals) or Head of the Infant and Junior School, for periods of up to five working days, and parents may be required to discuss the issues with the Deputy Head (Individuals), or Head of the Infant and Junior School, and their child before the item(s) is/are returned.
- NHS reserves the right to examine information held on phones and similar devices if there are reasonable grounds to suspect that school rules on using them have been broken. Two staff should be present if this is possible.
- Sanctions may be imposed on students who use their electronic equipment without consideration for others.

We expect all students to adhere to this charter for the safe use of the internet. Copies are available to students and their parents on the NHS web site. We may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices.

Education in E-Safety

Heads of Year are aware of the above e-safety issues and the school's PSHE includes sessions on e-safety. Working with the PSHE co-ordinator the Heads of Year educate the students as they move through the School in the risks and the reasons why they need to behave responsibly online. The DSL handles allegations of misuse of the internet. The PSHE programme in the IJS includes sessions on e-safety.

E-Safety is also delivered through Year Group and Whole School assemblies and is discussed during planned form time in smaller groups.

Misuse of the Internet

We will not tolerate any illegal material, and the DSL will always report illegal activity to the police and/or the Local Child Safeguarding Board (LSCB). If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any student who misuses ICT to bully, harass or abuse another student in line with our anti-bullying policy.

Involvement with Parents and Guardians

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact you if we have any worries about your child's behaviour in this area, and we hope that you will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. We

therefore arrange discussion evenings for parents when an outside specialist advises about the potential hazards of this exploding technology, and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

6. Use of Personal Data

Personal Data is used in line with our Data Protection Policy and Privacy Policies and Notices, published at https://nottinghamhigh.co.uk/policies.