

Procedure on Responsible Behaviour in Cyber Space

Procedure on Responsible Behaviour in Cyber Space

THIS POLICY INCLUDES THE EARLY YEARS FOUNDATION STAGE [EYFS]

Procedure on Responsible Behaviour in Cyber Space

Contents

1. Introduction	3
2. Internet	3
3. The Role of ICT in Our Pupils’ Lives.....	4
4. Role of NHS ICT Staff	4
5. Role of Our Designated Senior Lead	4
6. Responsible Use of the Internet and Electronic Devices at NHS	5
Cyberbullying	5
Sexting:.....	5
Treating other ICT users with respect.....	6
Keeping the School Network Safe.....	6
Promoting Safe Use of Technology	6
Safe Use of Personal Electronic Equipment.....	7
Considerate Use of Electronic Equipment	7
Education in E-Safety	7
Misuse of the Internet	8
Involvement with Parents and Guardians	8

Procedure on Responsible Behaviour in Cyber Space

The latest versions of the School's Safeguarding and Child Protection policies can be found at:

<http://www.nottinghamhigh.co.uk/about-us/school-policies>

Abbreviations used in this document: NHS = Nottingham High School, DSL = Designated Senior Lead.
GEP = General Education Programme, ICT = Information and Communications Technology

1. Introduction

This Procedure is concerned with pupils' responsible behaviour in cyber space. See also the NHS ICT 'Acceptable Use' policies.

Our ICT staff use the Child Exploitation and Online Protection centre (CEOP) ThinkUKnow resources for up-to-date guidance and materials which are cascaded to the DSL and other staff when appropriate.

2. Internet

Pupils are taught in lessons, through assemblies and GEP 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 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 pupils. The filtering system used in our school blocks inappropriate content whilst allowing the pupils a safe environment to learn. We currently filter out several social media sites, such as Facebook and Twitter.

Although pupils 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 pupils with 3G and 4G access to networks and will be alert to pupils 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,

Procedure on Responsible Behaviour in Cyber Space

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

3. The Role of ICT in Our Pupils' 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-enabled and Wi-Fi mobile phones, 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, GEP lessons and assemblies, to educate our pupils in how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, sexting, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment, hence 'over blocking' is not normal practice.

4. 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 pupils 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.

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 pupils or staff must be passed on to SMT.

Our ICT staff are aware of the guidance from the UK Safer Internet Centre: appropriate filtering and monitoring and also the guidance available from the National Education Network – NEN.

5. Role of Our Designated Senior Lead

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

The DSLs and DDSs are conversant with the safety issues involved with the misuse of the internet and other mobile electronic devices. 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

Procedure on Responsible Behaviour in Cyber Space

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 pupils in the school are not at risk.

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

6. 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.
- 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 pupils 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-16 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 pupils is available at:

www.thinkuknow.co.uk

<https://www.childline.org.uk/explore/onlinesafety/pages/sexting.aspx>

Advice for parents is available at:

www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting

Procedure on Responsible Behaviour in Cyber Space

Treating other ICT users with respect

- We expect pupils 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 and the expectations stated in the Essential Guide to Sixth Form which are published in the Student and Sixth Form Planners respectively.
- We expect a degree of formality in communications between staff and pupils and would not normally expect them to communicate with each other by text or mobile phones. Our policy on Educational Visits explains the circumstances when communication by mobile phone may be appropriate. In such circumstances, staff use School, as opposed to personal, mobiles and pupils' mobile numbers are deleted at the end of the visit. Pupils 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 set out in the Student and Sixth Form planners and is also published on the website.
- All pupils 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.

Keeping the School Network Safe

- Certain sites are blocked by our filtering system and our ICT Department monitors pupils' use of the network.
- The ICT Department monitors email traffic and blocks SPAM and certain attachments.
- We issue all pupils 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

Pupils 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)

Procedure on Responsible Behaviour in Cyber Space

As mentioned previously, ICT assemblies and GEP 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 GEP lessons.
- Our GEP lessons include guidance on how pupils 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.

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 (Pastoral) 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 (Pastoral), 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 pupils who use their electronic equipment without consideration for others.

We expect all pupils to adhere to this charter for the safe use of the internet. Copies are given to all pupils in the Senior School and are available to 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 GEP includes sessions on e-safety. Working with the GEP co-ordinator the Heads of Year educate the pupils as they move through the School in the risks and the reasons why they need to behave responsibly online. The

Procedure on Responsible Behaviour in Cyber Space

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 pupil who misuses ICT to bully, harass or abuse another pupil 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.