Autumn 15

eSafety Policy

This policy should be read in conjunction with the following policies:

1 Safeguarding Policy
2 Child Protection Policy
3 Anti-bullying Policy
4 Positive Behaviour Policy
5 Acceptable use of hand-held technology and the Internet for students Policy (AUP)

Hazelwood Integrated College
70 Whitewell Road, Newtownabbey, BT36 7ES telephone 028 9077 4202

SUMMARY:

This policy aims to layout the conditions of use, for students, in regard to ICT networked resources including: Internet access, Email, devices, and the College Virtual Learning Environment (VLE) both inside and outside of the College.

Students are expected to use ICT resources in a responsible manner consistent with the College ethos and Code of Conduct.

T. Jamison

E-Learning Coordinator

October 2015

• New policy for the College

• Incorporates recommendations by the Department of Education in DE Circulars "eSafety Guidance 2013/25" and "Preventing Child Sexual Exploitation, June 2015".

• Written after consultation with Child Protection Officer, Network Manager & E-Learning coordinator.

• It is the schools responsibility to have a policy in place that provides guidance on acceptable use of the Internet & eSafety.

ADDITIONAL NOTES

Policy Number: 2015/10 (draft)

HISTORY:

Drafted: October 2015

Ratified: January 2016

Amended by E-Learning Coordinator

E-Mailed to Principal:

Circulated to Parents for ratification:

eSafety Statement.

This draft policy is new to the college and has been developed in conjunction with the Child protection, Acceptable use & Anti-bullying policies. This draft, October 2015, takes account of DENI guidance on "eSafety Circular Number: 2013/25" and "Preventing Child Sexual Exploitation, June 2015".

We in Hazelwood College have a primary responsibility for the care, welfare and safety of the students in our charge. It is our aim to provide a safe, healthy, caring and supportive school in which each individual can learn and develop to their full potential. It is also recognized that all teachers, supported by our ancillary and secretarial staff, have a role to play in safeguard our students from the dangers of online abuse, harassment and exploitation.

Our commitment is to provide a safe environment that promotes an awareness of online dangers. We commit developing students' self-discipline and providing them with the skills and qualities to protect themselves and remain safe online.

It is the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. eSafety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

Rationale

As an integral part of pupils' lives, both inside and outside school the Internet offers many positive opportunities for our students to learn and communicate online with their peers, in relative safety. However students should be aware of the dangers presented including violence, racism and exploitation from which pupils need to be reasonably protected.

The college aims to teach students how to learn to recognise and avoid these risks, to become "Internet-wise" and ultimately good "digital citizens". Students should be confident in what to do if they come across inappropriate material or situations online.

Aims

- To safeguard our students in the digital world to enhance learning to understand and use new technologies in a positive way; focusing on education about the risks and the benefits so that students feel confident online;
- To support students in their development of safer online behaviours both in and out of school.

Guidance

Inappropriate use of the internet and mobile technologies, such as trolling, sexting, cyberbullying or sexual exploitation can have a devastating impact on the lives of our children and young people.

The college's advice is as follows:

- Don't share personal information or images with people you don't know.
- Don't accept friend requests with someone you don't know – not everyone online may be who they say they are.
- Set privacy settings on all devices so that only people you know can view your account.
- Don't post anything online that you are not happy to be shared, particularly nude or nearly nude images or videos. There is the risk that these images could be shared or get into the wrong hands and could lead to harmful situations such as stalking, abuse or blackmail. It is a crime to possess, take, make, distribute or show anyone an indecent or abuse image of a child or young person under 18 years of age.
- People may wish to abuse, exploit, intimidate or bully you online, if someone has made you feel uncomfortable or you have had disturbing interaction, tell someone immediately, preferably the police or a trusted adult.
- If you receive any inappropriate images or links, it is important that you do not forward it to anyone else. Contact police or tell a trusted adult immediately. By doing this you could help prevent further such incidents. You will not get into trouble.

Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying should be considered within the schools overall anti -bullying policy and pastoral services as well as the eSafety policy.

Care should be taken when making use of social media for teaching and learning. Each of the social media technologies can offer much to schools and pupils but each brings its own unique issues and concerns. Each social media technology that is to be utilised should be risk assessed in the context of each school situation.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites (like Facebook & Twitter) – typically includes the posting or publication of nasty or upsetting comments on another user's profile.

- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997 http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988 http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003 http://www.legislation.gov.uk/ukpga/2003/21

It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Schools should also keep good records of cyber-bullying incidents to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

Grooming and images of child abuse

If school staff, parents or pupils suspect or are made aware of the following illegal acts it must be reported to the Designated Teacher immediately.

- A child under 16 enticed or coerced to engage in sexually explicit conduct on-line.
- Importing or transporting indecent images of children using telecommunications public networks.
- Knowingly receiving images of child abuse whether via the internet or other digital device (e.g. mobile phone)
- Images which appear to be photographs whether made by computer graphics or otherwise are also covered under Sexual Offences legislation.

Roles and Responsibilities.

All members of the College have responsibility to challenge and or report an eSafety incident. In the first instance members of staff should use their professional judgement and deal with or report the incident to tutor, HOY or CPO.

If you suspect there is a child protection issue it should be raised immediately to the designated teacher or Principal, in the case of a critical issue.

If you suspect a mobile device contains sexually explicit images of a child (under 18 years of age) it should be passed directly to the designated teacher.

Do not view, save and send any image as you may be committing an offence.

External support Agencies

Contact PSNI on 101 or for help and advice ring Childline on 0800 1111 or Lifeline on 0808 808 8000.

Go to www.getsafeonline.org for lots of useful advice and information on how to stay safe online. Safeguardingni.org will also provide information for parents and carers on e-safety.

Links to other sites that can provide information and advice to young people and parents are available from the DE website at: http://www.deni.gov.uk/index/pupils-and-parents/pupils.htm

Childnet International is a non-profit organisation working to "help make the Internet a great and safe place for pupils". Childnet have produced many materials to support the teaching of eSafety at Key Stage One and Two. They have also produced materials for parents, staff and post primary pupils. Their materials are available to access online or order from www.childnet.com.

Training and Support

Teachers are the first line of defence in eSafety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to illegal activity.

Staff should avail of training and support to determine what action is appropriate including when to report an incident of concern to the school Designated Teacher for Child Protection or the member of Senior Management with responsibility for eSafety.

eSafety training should be an essential element of staff induction and should be part of an on-going Continuous Professional Development programme. A clear and effective eSafety policy should can ensure that all reasonable actions are taken and measures put in place to protect all users.

Detailed advice and guidance on eSafety is available to teachers within an eSafety Zone, via the C2k exchange. C2k will be offering training and support in the entire area of eSafety to all schools during the coming year.

Child Exploitation and Online Protection (CEOP) resources are a useful teaching tool for all Key Stages looking at Internet safety and can be usefully incorporated into a PDMU/LLW or ICT programme. ***www.thinkuknow.co.uk*** **.**

Review

The eSafety Policy will be regularly reviewed as part of the policy review cycle.