NEW HORIZON COMMUNITY SCHOOL

E-Safety Policy

2018-2019

Updated: January 2019
Date of next Review: November 2019

Introduction

Protecting young people in the online world means thinking beyond the school environment. As well as the computer to access the Internet, now many mobile phones and games consoles offer broadband connections. Pupils may be working online in school, at home or in an Internet café. Increasingly pupils will have access to personal devices not covered by network protection and therefore the emphasis needs to be on educating all users as to the risks involved and their obligation to act responsibly while online.

Safeguarding pupils in both the real and virtual world is everyone's responsibility and all staff should be aware of this policy and how to respond to e-safety incidents.

All pupils should be made aware of the school's Acceptable Use Policy (AUP) and what to do if they have any ICT safeguarding concerns. Harassment, grooming of another person using technology, breaching their right to privacy, poses a serious threat to physical and emotional safety, and may have legal consequences.

Procedures for dealing with Inappropriate / Illegal Internet Access or Material

If staff or pupils discover unsuitable websites, this should be immediately reported to the CPO who, in liaison with the ICT teacher for the school, will consider a referral to the Internet Watch Foundation (IWF) and the Police. Illegal material within the school's network is a very serious situation and must always be reported to the Police. Our school ensures processes are in place to minimize the risk of students gaining access to inappropriate materials, through supervision and monitoring. Any incident that involves inappropriate adult access to legal material on the school premises will be dealt with by the school's disciplinary policy.

In the event of discovery of illegal material seek immediate and specific advice from the CPO who will consult with the ICT teacher, the Head teacher and the Police.

Combating Cyber-bullying

Cyberbullying is a form of bullying and can be defined as 'the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately and over a period of time, to upset someone else'. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying:

the invasion of home and personal space; the difficulty in controlling electronically circulated messages, the size of the audience, perceived anonymity, and even the profile of the person doing the bullying and their target. The School Rules and Regulations state that “misconduct of any kind outside of School will be amenable to School discipline if the welfare of another pupil or the culture or reputation of the School is placed at risk.” Our role with regards to Bullying and Cyberbullying can extend therefore beyond the “School gates” and may include times when pupils are not under the control or charge of a member of staff.

Cyberbullying takes different forms: threats and intimidation, harassment or 'cyber-stalking' (eg repeatedly sending unwanted texts or instant messages), vilification / defamation; exclusion or peer rejection, impersonation, unauthorised publication of private information or images and manipulation.

Some cyberbullying is clearly deliberate and aggressive, but it is important to recognise that some incidents of cyberbullying are known to be unintentional and the result of simply not thinking about the consequences. What may be sent as a joke may not be received as one, and indeed the distance that technology allows in communication means the sender may not see the impact of the message on the receiver. There is also less opportunity for either party to resolve any misunderstanding or to feel empathy. It is important that pupils are made aware of the effects of their actions.

In cyberbullying, bystanders can easily become perpetrators, eg by passing on or showing to others images designed to humiliate, or by taking part in online polls or discussion groups. They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the person targeted. Our policy is clear: 'bystanders' — better termed 'accessories' in this context — who actively support cyberbullying should expect a sanction for this behaviour. It is important that pupils are aware that their actions have severe and distressing consequences, and that participating in such activity will not be tolerated.

There are particular features of cyberbullying that differ from other forms of bullying which need to be recognised and taken into account when determining how to respond effectively. The key differences are:

- **Impact** — the scale and scope of cyberbullying can be greater than other forms of bullying.
- **Targets and perpetrators** — the people involved may have a different profile to traditional bullies and their targets.
- **Location** — the 24/7 and any-place nature of cyberbullying.

- **Anonymity** — the person being bullied will not always know who is attacking them.
- **Motivation** — some pupils may not be aware that what they are doing is bullying.
- **Evidence** — unlike other forms of bullying, the target of the bullying will have evidence of its occurrence.

Prevention

We seek to instill values in all members of the school which should, preclude bullying. These are reinforced by a PSHE and religious programme which requires staff at all levels of the School to spend time talking to their groups about cyber bullying and its effects and consequences. In essence, these seek to inculcate respect for others, their property and their individuality. The above values should not only be addressed in PSHE and Islamic subjects but should also underpin ordinary curricular lessons, assemblies, Horizons Lectures, tutorials, debates, the co-curricular programme .

It is crucial to the School's success in dealing with cyberbullying that all members of the community are made aware that it is unacceptable and should not be tolerated. It is the responsibility of all members of the community to take action if they are aware of it happening. To remain silent is to condone the action of the bully. Staff should receive regular training and guidance in order to reduce the risk of bullying arising particularly at times or in areas where it is most likely. If necessary, external agencies will be consulted if specialist skills may be required.

Procedure

1. Information about bullying comes from a variety of sources, including parents, pupils, staff and members of the public. In all cases we assure the person making the allegation that we shall be taking immediate action to stop the bullying / cyberbullying and will pursue information so as to identify the bully. Parents are informed as soon as possible, though sometimes some leeway may be required in order for investigations to be completed.

2. Depending on the nature of the allegation, the case will be taken up either by the Head teacher, form tutor, other staff or a combination of these people. As a rough guide, the more serious the allegation, the more likely it is to involve senior staff. If there is a Child Protection implication, i.e. if there is reasonable cause to suspect that a child is suffering, or likely to suffer significant harm then the Child Protection Officer **must** be informed.

3. Interviews will be conducted fairly, giving all sides the opportunity to state their case, so as to establish the truth in what seldom turn out to be straightforward

issues. In all cases, pupils will be warned not to do or say anything that may prejudice their position vis-à-vis the pupil who has been bullied. (No revenge / stirring up support among friends, no taking the law into their own hands.)

4. Except for the most straightforward cases, in which truth has been established and the matter has been resolved swiftly, an interview will be conducted; a pupil would be invited to bring a friend or member of staff to support them in any such interview. This will enable a record to be kept of the interview and what is said to be corroborated. Notes, both rough copies and, where necessary, a brief summary and copies of any letters sent to parents will be put on files with cross referencing where appropriate. Notes will be retained by the Head which will enable patterns to be identified.

5. Letters written to parents will detail the nature of the offence and any sanctions imposed, and will set out what improvements the School expects to be made in behaviour as well as the consequences of failure to improve.

6. At the conclusion of the investigation, if appropriate, one of the members of staff involved will contact parents of all pupils directly involved and inform them of action taken. Wherever possible, the identity of "informers" and pupils other than the son or daughter of the parent will not be disclosed.

7. In practice, the sanctions applied range from a verbal warning or a ban on use of the School's computer network, to temporary or permanent exclusion, depending on the gravity of the offence and the pupil's previous record with reference to bullying.

Sanctions for Cyberbullying Behaviour

In practice, the sanctions applied range from a verbal warning or a ban on use of the School's computer network to a temporary or permanent exclusion, depending on the gravity of the offence and the pupil's previous record with reference to bullying / cyber-bullying. In the most severe cases, it can result in criminal prosecution.

The aim of sanctions is to:

- Help the person harmed to feel safe again and be assured that the bullying will stop.
- Hold the perpetrator to account getting them to recognise the harm caused and deter them from repeating the behaviour.
- Demonstrate to the school community that cyberbullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly.

When cyberbullying is investigated, reference will be made to the Acceptable Use Policy (AUP); sanctions for breaches are set out in the AUP and the 'Procedure for dealing with Bullying / Cyberbullying incidents'. Technology-specific sanctions for pupils engaged in cyberbullying behaviour could include limiting internet access for a period of time or removing the right to bring a mobile phone into school (although issues of child safety will be considered in relation to the latter).

Cyberbullying will have an impact on the education and wellbeing of the person being bullied, and the physical location of the bully at the time of their action is irrelevant in this. Schools have broad powers to discipline and regulate the behaviour of pupils, even when they are off the school site. Misconduct of any kind outside of school will be amenable to school discipline if the welfare of another pupil or the culture or reputations of the school are placed at risk.

Anti-Cyber-bullying Code: Advice to pupils

Being sent an abusive or threatening text message, or seeing nasty comments about yourself on a website, can be really upsetting. This code gives you seven important tips to protect yourself and your friends from getting caught up in cyber-bullying, and advice on to how to report it when it does happen.

1. Always respect others

Remember that when you send a message to someone, you cannot see the impact that your words or images may have on the other person. That is why it is important to always show respect to people and be careful what you say online or what images you send. What you think is a joke may really hurt someone else. Always ask permission before you take a photo of someone.

If you receive a rude or nasty message or picture about someone else, do not forward it. You could be assisting a bully and even be accused of cyber-bullying yourself. You could also be breaking the law.

2. Think before you send

It is important to think before you send any images or text about yourself or someone else by email or mobile phone, or before you post information on a website. Remember that what you send can be made public very quickly and could stay online forever. Do you really want your teacher, parents or future employer to see that photo?

3. Treat your password like your toothbrush

Don't let anyone know your passwords. It is a good idea to change them on a regular basis. Choosing hard-to-guess passwords with symbols or numbers will help stop people hacking into your account and pretending to be you. Remember to only give your mobile number or personal website address to trusted friends.

4. Block the Bully

Most responsible websites and services allow you to block or report someone who is behaving badly. Make use of these features, they are there for a reason!

5. Don't retaliate or reply

Replying to bullying messages, particularly in anger, is just what the bully wants.

6. Save the evidence

Learn how to keep records of offending messages, pictures or online conversations. These will help you demonstrate to others what is happening and can be used by your school, internet service provider, mobile phone company, or even the police to investigate the cyber-bullying.

7. Make sure you tell

You have a right ***not*** to be harassed and bullied

online. There are people that can help:

- Tell an adult you trust who can help you to report it to the right place, or **call ChildLine on 0800 1111** in confidence.
- Tell the provider of the service you have been bullied on (eg your mobile-phone operator or social-network provider). Check their websites to see where to report.
- Tell your form tutor, or any member of staff will support you and can discipline the person bullying you.

Finally, don't just stand there. If you see cyber-bullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?

3.9 E-Safety Document

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult their schools e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use this schools' ICT system for a purpose not permitted by New Horizon Community School.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised systems manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-safety coordinator, the designated child protection / head teacher
- I will ensure that electronic communication with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and I will help them to develop a responsible attitude to system use, communications and publishing.
- New Horizon Community School may exercise its right to monitor the use of the school's ICT systems to intercept email and delete inappropriate materials where it believes unauthorised use of the schools information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Name (Print): …… Sign:…… Date: …….

Accepted for School (print): …… Sign:……