DROYLSDEN
Academy

E-Safety Policy

Reviewed: Every 2 Years
Next Review Date: February 2025
Person Responsible: Assistant Headteacher T & L & ICT
Approving Body: Headteacher

The Four Cs

The DfE's 2022 'Keeping Children Safe in Education' (KCSIE) statutory guidance states that "Online safety and the school or college's approach to it should be reflected in the child protection policy. Considering the 4Cs (Content, Contact, Conduct and Commerce) will provide the basis of an effective online policy." We address these aspects of Child Protection within our E Safety Policy.

Phone Policy

In order to keep our students safe, the Academy employs a strict attitude to student's phones. Student's phones must not be seen or heard. If a student is found using their phone in school it will be confiscated and locked in a safe. Home will be contacted to collect the phone. If home 5
is not able to willing to collect the phone it will be returned to the student at the end of the week. All students entering Navigation must hand over their phones and will receive them back at the end of the day.

Cyber Bullying

We as an Academy take all forms of bullying seriously and this includes Cyber Bullying. Cyber Bullying is defined as using any form of technology to abuse or threaten another person.

Examples include:

- Sending harassing text messages
- Making malicious/abusive phone calls
- Taking a picture/video of people on mobiles and passing these around for amusement
- Writing threatening E-mails
- Being abusive in chat rooms
- Writing nasty things about people in websites
- Sending nasty instant messages
- Breaking into someone's e-mail account to send nasty messages to others
- Standing by and watching others do any of the above

What will Droylsden Academy do?

- Make sure that cyber bullying is understood by all staff and added to your anti-bullying policy.
- Ensure all Academy staff, pupils and parents know about the policy and systems and that they are regularly updated.
- Monitor internet traffic within the Academy.
- Ensure that cyber bullying is taught as part of a balanced PSHE curriculum and ensure it teaches pupils how to be safe on the internet and on their mobile phones, demonstrating the pros and cons of each.
- Introduce clear policies on use of mobile phones in Academy and during Academy activities.
- Regularly inform staff of new technologies and ways in that they might be abused by people intent on causing harm to others.
- Ensure harmful websites are blocked and regularly check that this remains the case.
- Provide parents with a list of blocked sites and reasons for blocking every term.
- Work with police and other partners such as voluntary agencies e.g. Childline on managing cyber bullying.

What can parents do?

- Take an interest in what your child is doing on the computer.
- Familiarise yourself with the websites that your children uses.

- Read carefully the information from your Internet Service Provider (ISP) about setting parental controls and use them.
- Monitor what sort of sites your child visits most and ask them what they are doing. If your child was going out, you would ask what they were doing and where they are going, this is the same thing!
- Understand what is meant by the different terms that people use in chat rooms.
- Familiarise yourself and your children with www.internetsafetyzone.com. Discuss the issues, concerns and safety features with your child.
- If your child does want to meet someone from a chat room, make sure you accompany them and that they know the risks.
- Contact the Academy at any time to voice any concerns you may have over what your child is doing. (161 301 7600)

What can young people do?

- If in chatrooms, always use a nickname, don't give people you don't know your personal information like full name, mobile number etc. You wouldn't do this straight away on the street, so why do it online?
- Be very careful about what kind of picture, if any, you post onto the internet as people could alter it and use it for other purposes.
- If you are being harassed on-line, report this abuse via the link on the website and leave the area (i.e. chat room, instant messaging).
- If you receive nasty messages through e-mail or IM, block the sender and report them to the website. Never reply to harassing messages.
- Never meet a chatroom buddy in the real world without a trusted adult accompanying you first - better safe than sorry!
- Remember, not everyone on the Internet is who they say they are. It is like meeting a stranger in the street, you would not believe everything they tell you at first, would you?

Responding to incidents of technology misuse:

Even with all the policies and technological solutions in place, there may still be occasions when misuse of the internet and related technologies occur. Therefore, we must have appropriate strategies in place for responding to such instances.

Senior managers in schools are required to respond to a wide variety of incidents on a daily basis. Most of these incidents are minor, but some are more serious. The majority involves students, but on occasion it may be a teaching or non-teaching member of staff whose conduct is in question. Schools generally work from procedures which are based on school policy and established practice to deal with such incidents. However, responding appropriately to a breach of internet safety can cause some uncertainty, sometimes over what the nature of the offence may be, or even because of a lack of understanding of the potential seriousness of incidents involving ICT.

This section provides some examples of ICT-related incidents which schools might encounter, and suggests some strategies for dealing with them.

Minor incidents of technology misuse:

Minor incidents of misuse by pupils might include:

- Copying information into assignments and failing to acknowledge the source (plagiarism and copyright infringement)
- Downloading materials or images not relevant to their studies, in direct breach of the Academy's acceptable use policy

- Misconduct associated with student logins, such as using someone else's password
- Incidents involving pupils using their own technology in the Academy, such as having a mobile phone on their person (whether turned on or not), using it in class, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving.

In all but the most minor of cases it would be wise for the pupil to be issued with a warning, and the incident documented. If the behaviour is repeated, or the misconduct escalates, it can then be responded to more seriously if the Academy has evidence of previous events. Any incident of racially motivated abuse via technology needs to be linked in with the monitoring of racial incidents in the Academy and reported in the necessary way.

The internet safety co-ordinator should monitor minor incidents to identify trends in pupils' behaviour, and should react proactively to any emerging issues. This might include raising awareness on a particular internet safety topic at an Academy assembly or offering staff additional training. It is also wise to periodically review the Academy's internet safety policies, and, in particular, acceptable use policies, to see if they should be modified in any way.

Incidents involving inappropriate materials or activities:

While not illegal, there will be some material that is just not appropriate within the Academy environment, and, in the case of staff, not in keeping with the professional standards or code of ethics of those who work with children and young people.

Examples might include soft-core pornography, hate material, drug or bomb-making recipes, or material that others may find offensive such as sexist or racist jokes, cartoons, or material which is used in low-level harassment. Specific breaches of policy and rules might include deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the Academy's network.

Even if such material was not deliberately accessed by the pupil, but not reported to a teacher, and was subsequently shown to other students, this should also merit a disciplinary response. Other incidents of more serious misuse by pupils might include cheating in an examination or plagiarism in coursework, which, aside from infringing Academy assessment policies, may have legal implications (for example, they may breach copyright law). Hacking, virus attack, chronic truancy (as a result of obsessive or excessive use of the internet and related technologies) and online gambling are all serious concerns for schools, and require a disciplinary response.

Age-restricted material is potentially more serious. Publications are classified to provide information and protect people from viewing material that might be inappropriate or damaging to their moral and physical wellbeing. It is therefore illegal to show, give or sell restricted materials to a person under a certain age. Blatant, intentional exhibiting of age-restricted materials to pupils under the specified age is a serious breach of internet safety and should invoke a strong disciplinary response from the Academy.

Any incident involving a member of staff is a serious, and often complex matter. There may be implications for the safety of pupils, fellow employees and the learning environment, and for the reputation of the Academy. We need to, therefore, ensure that all members of staff are aware of and have signed the acceptable use policy. This ensures that policies and procedures are in place should incidents occur.

Harassment of another person using ICT, or breaching their right to privacy, poses a serious threat to their physical and emotional safety, and again may have legal consequences. More serious incidents relating to internet safety in schools should be reported to the internet safety co-ordinator immediately. The internet safety co-ordinator must document the incident and decide on an appropriate course of action, which may

include involving the Headteacher and external agencies. It may also be necessary to involve child protection staff to provide follow-up counselling and support to both the victims and perpetrators.

The internet safety co-ordinator should review internet safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing Academy-wide training as appropriate. This includes liaising with the network manager to ensure that any such sites etc are blocked.

Incidents that involve inappropriate but legal material should be dealt with by the Academy via the usual disciplinary system; unless a criminal offence has been committed, it is not normally necessary to involve the police. Depending on the nature of the incident there may be breaches of other Academy policies, such as the anti-bullying policy.

Disciplinary action may range from a warning to dismissal of a staff member or suspension of a pupil. As in all disciplinary instances of this seriousness, an Academy must be careful to follow disciplinary protocols, ensuring that proper documentation and recording of information occurs, and that appropriate counselling and support are given, and ensuring that parents and carers of the pupil involved are kept fully informed of the matter. If police involvement is necessary, it is advisable for the Headteacher to seek legal advice, via the LEA, as soon as possible.

We have now set a precedent at Droylsden Academy that any student found to be viewing or downloading hard-core pornographic material in school will be suspended for three days and banned from using the computers for four weeks.

Any serious incidents could become the subject of media attention. We need to ensure that we have an appropriate strategy in place for dealing with media requests, and ensure that ongoing investigations and the continuing safety of the Academy are not compromised by media coverage.

Incidents involving illegal materials or activities:

In the Academy context, very serious incidents tend to involve illegal materials (particularly the viewing, possession, making and distribution of indecent images of children) or serious stalking or harassment facilitated by communication technologies. Such criminal offences may be committed by staff and pupils alike. Indecent images of children are defined under Section 7 of the Protection of Children Act 1978 (as amended by Section 84 of the Criminal Justice and Public Order Act 1994). References to indecent photographs under the Act include data stored on a computer disk or by other electronic means that is capable of conversion into a photograph.

The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar unsocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which he/she knows, or ought to know, amounts to harassment of the other. Although the term is deliberately not defined in the Act, words such as ‘alarm’, ‘distress’ or ‘torment’ fit the term most accurately, and some adverse impact on the victim is required. To constitute a ‘course of conduct’, harassment must take place on a minimum of two occasions.

Discovery of indecent material within the Academy’s network is a very serious situation, and must always be reported to the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, we must do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but we do not do this unless instructed by the police. We must ensure that everyone is kept away and that nothing is touched.

Under no circumstances should the internet safety co-ordinator, network manager or Headteacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases, this may constitute a criminal offence in itself.

In cases of pupil or staff involvement with indecent materials, it would be sensible for the Academy to seek legal advice as soon as possible, particularly with regard to the disciplinary actions that are acceptable while the police carry out their investigations.

In the event of a very serious incident occurring within the Academy, it is essential that a review of all internet safety policies and procedures is conducted as soon as possible. The Headteacher would have ultimate responsibility for the review process, but would probably delegate this to the internet safety co-ordinator and the Academy's internet safety team. The three key components of a safe ICT learning environment (the infrastructure of whole-academy awareness, designated responsibilities, policies and procedures; the effective range of technological tools; and a comprehensive internet safety education programme) should also be reviewed, ensuring that:

- Comprehensive debriefing occurs after the incident to maximise what can be learnt
- The network manager has the professional skills to carry out regular safety checks, and knows the correct protocols to follow if illegal material is suspected or encountered
- All Academy staff understand the circumstances under which a forensic audit of computers should be carried out, and by whom, and the appropriate strategies to adopt to ensure that evidence is secured and preserved (see Appendix 4 for further information)
- The Academy's internet safety team (both policy and management) contains staff with all the relevant expertise, and that the appropriate time and authority is allocated to the team to allow them to carry out their duties effectively. Further information on illegal content – including when, where and how to report it – can also be found on the Internet Watch Foundation website [http://www.iwf.org.uk].

Incidents involving students who are looked after (CLA):

Students who are CLA may come to you to discuss e-contact that has been made with them by their birth families. Always report this to the child's foster carers and social worker.

- Assure student that they have done nothing wrong
- Collate all evidence
- Pass information to Social Worker and Foster Parents
- Offer e-safety training to foster family and young person if required

This policy was adapted from the Becta publication "E-safety, developing whole-school policies to support effective practice"

Flowchart for responding to Internet Safety incidents in the Academy

Internet Safety Incidents:

If Illegal Materials or Activity is Found (or Suspected), depending on the severity the Academy may conduct the following actions:

- Report to Internet Safety Co-ordinator and/or Head Teacher
- Report to Police
- Secure and Preserve Evidence
- Await Police Response
- If illegal material or activity is confirmed: allow police to complete their investigations seeking advice from LEA on interim treatment of staff member or pupil.
- If no illegal material or activity is confirmed:

- Revert to Academy disciplinary procedures for staff member or pupil
- If pupil: review incident, treat as per policy and take appropriate action including blocking account for a minimum of a week and informing parents/carers
- If staff: review incident, treat as per policy and take appropriate action
- Record Incident on Internet Safety Incident Form
- Review Policies and technical tools
- Implement Changes
- Monitor

Useful Links:

www.thinkuknow.co.uk
www.childline.org.uk
ww.iwf.org.uk

Keeping Children Safe in Education 2022

Child Exploitation and Online Protection

Department for Education - Advice for Parents and Carers on Cyberbullying A Parent's Guide to Dealing with 'Sexting'

Contact Numbers:

Childline - 0800 1111
Samaritans - 08457 909 090
NCH - Text 'BULLY' to 60000