Academic Guardians UK

ONLINE SAFETY (E-SAFETY)

Policy	Online Safety (E-Safety)
Summary	This policy links to the Academic Guardians Safeguarding and Child Protection Policies and outlines how we ensure that we maximise the safety of our students who use the internet and related communication technologies. The good practice in this policy content is aligned to the requirements of Keeping Children Safe in Education 2016.
Policy Owner	Andrew Kettle (DSL) Update: March 2018
Next Review Date:	March 2019

1 Policy Introduction

1.1 The use of the internet and online social networking sites is now very much a part of everyday life for education and social interaction. Students frequently engage with the internet inside and outside of school. However, the increase in use of the internet and social networking sites through the use of mobile devices has raised concerns about online safety with particular reference to abuse, cyber bulling and grooming. Concerns include being exposed to illegal or inappropriate material online, being subject to harmful interaction i.e. cyber bullying and grooming, as well as a child's conduct on the internet that may increase their chance of harm i.e. posting personal information on the internet. The potentially dangerous uses of the internet can also take place outside of school, though issues often manifest in schools and we understand the need to respond swiftly and confidently to ensure that all students are safeguarded, supported and educated in the safe use of the internet. This policy provides a guide for staff, students' parents and homestay host families as to how Academic Guardians UK will educate and promote safety and wellbeing and what steps will be taken should a safeguarding concern be reported or suspected. Our response to these incidents will be the least intrusive response appropriate to the risk, maintaining the primary concern being the welfare and protection of the young people involved.

1.2 This policy forms part of the Academic Guardians UK safeguarding arrangements and all reported incidents will be dealt with as safeguarding concerns. It is based on the NSPCC advice for 'Online Safety', and the 'Keeping Children Safe in Education' guidance and should be read in conjunction with the following AGUK policies: Safeguarding and Child Protection, Youth Produced Imagery Policy and Child Sexual Exploitation Policy.

2 What is 'online abuse'

2.1 Online abuse is characterized as abusive behavior mediated by online platforms which include social networks, playing online games, and using mobile phones. The NSPCC have identified five forms of online abuse that young people may experience. These include:

2.1.1 Cyberbullying

- Abusive comments, rumors, gossip and threats made using digital communications and/or technologies this includes internet trolling.
- Sharing pictures, videos or personal information without the consent of the owner and with the intent to cause harm or humiliation.
- Hacking into someone's email, phone or online profiles to extract and share personal information, or to send hurtful content while posing as that person.
- Creating dedicated websites that intend to harm, make fun of someone or spread malicious rumors.
- Children may be aware of their cyber bullier, and this may be an extension of offline bullying. However, the ease of anonymity online increases the likelihood bullying.

2.1.2 Grooming

- Building an emotional connection with a child to gain their trust for the purposes of sexual abuse, exploitation, or trafficking

2.1.3 Sexual abuse

- A child is sexually abused when they are forced or persuaded to take part in sexual activities.

2.1.4 Sexual exploitation

- Sending or posting sexually explicit images. Please refer to the Youth Produced Imagery Policy.

2.1.5 Emotional abuse

- Emotional abuse is the ongoing emotional maltreatment of a child. It is sometimes referred to as psychological abuse and can seriously damage a child's emotional health and development

3 Academic Guardians UK Procedure for teaching and learning about E-Safety

3.1 Academic Guardians UK staff, students, parents and host families are encouraged to read and familiarise themselves with the various AGUK handbooks, policies and procedures outlining our advice regarding online e-safety.

3.2 All AGUK staff, homestay host families & drivers understand the risks posed to children in their care of exposure to online abuse.

3.3 The Designated Safeguarding Lead has the appropriate training and understanding to educate, promote and support the members of the organiastion, as well as best support the safeguarding of children in their care.

3.4 Useful guidelines for parents, host families, students, and staff can be found from The Child Exploitation and Online Protection (CEOP) body's online safety center https://www.thinkuknow.co.uk/

4 Advice for students

4.1 Students are advised to behave in accordance with the online e-safety policy of their school, regarding mobile and internet use, when both in and out of the school, i.e. staying with homestay host families.

4.2 Students must act responsibly when using the internet and additional advice and support is provided in this policy as well as the student handbook supplied by AGUK at the time of student registration. AGUK recommends all students to comply with the age restrictions in place on each social media site and strongly advocates the use of full privacy settings on all social media sites, to keep all personal information and photographs as private as possible.

4.3 During homestay visits, students must not use the internet for any illegal or inappropriate activity. This includes:

- Any 18+ sites i.e. pornographic or gambling sites.
- Downloading unlicensed material i.e. TV programmes, games, music, videos, and PDF files.

5 Social networking sites:

5.1 Since the use of computers and the internet is integral to the UK education system, it is essential to establish a safe internet environment during homestays. Homestay host families will be directed to the online safety policy of the relevant school for the student they are hosting. They should read and apply the recommendations of the school policy to the students under their care at that time.

5.2 During the application and recruitment process, homestay host families are guided through making their home e-safe for students, including networks, firewalls, privacy settings, appropriate use of filters and general time usage. Further Guidance on how to do so can be found on the NSPCC online safety site https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/parental-controls/. Host families should consider the number of students they are hosting, and their relevant ages and monitor how often their students are accessing to internet. Guidance on the appropriate internet use for different age groups can be found on the CEOP's 'think u know' guidance page https://www.thinkuknow.co.uk/

5.3 Homestay host families should refer to and follow the guidance implemented in the Homestay Host Family handbook and relevant polices made available to them, on an ongoing basis. From time to time AGUK also send out bulletins to relay important information regarding potentially dangerous online applications.

5.4 Social networking sites:

5.4.1 Homestay host families should be aware that their students might frequently use social networking to keep in contact with friends and families. They should ensure that students under their care understand the report and block functions on relevant sites and be strongly encouraged to keep their information private.

5.4.2 Guidance on frequently used social networking sites can be found through the NSPCC's Net Aware site. Homestay host families should refer to this, to stay up to date with the current concerns and privacy recommendations and can do so at https://www.net-aware.org.uk/

5.4.3 Homestay host families should talk to their students, promoting responsible behaviour, when they are using the internet and social media. If homestay host families suspect the student is being bullied they should encourage the child to speak to somebody and provide support. Guidelines for noticing online abuse or bullying in children can be found from the NSPCC, characterised by a change in behaviour. These changes in behaviour include:

- A drastic reduction in the amount of time spent using internet devices
- New phone numbers, email address, or contacts through frequently used applications that have not been noticed before
- An abnormally secretive attitude regarding their mobile phone or internet use, alongside being upset after using these programmes
- Trouble sleeping
- Low self-esteem and an avoidance of social situations that was not there previously

5.4.4 Signs of abuse must be reported to Academic Guardian UK staff, which will be dealt with in a procedural manner outlined in section 7 of this document.

5.4.5 Academic Guardians UK is aware that students can become friends of the homestay host families and keep in touch after the homestay. Contact of this form through social media sites and the internet must be thoughtful and appropriate.

6 Storage of information and data

6.1 Changes to Data Protection Law and the introduction on new General Data Protection Regulation (GDPR) law (May 2018) now mean staff, students, parents, homestay host families and drivers must ensure that all data and information is stored using the guidance provided in the AGUK Staff Handbook and Safeguarding Policy. The use of memory sticks/hard drives and cloud based storage is not permitted without authorisation, a full understanding of the risks to this data, appropriate permission levels granted for the use of the data in question.

7 Academic Guardians UK procedure for dealing with reports of online abuse

7.1 AGUK staff member receives the report of suspected online abuse from a student, parent, homestay host family or other source by face to face disclosure, email or telephone call.

7.2 AGUK Staff member adheres to the Child Protection Policy including recording the disclosure in the most appropriate format (using the Tell Explain Describe model if the information is being given by a student).

7.3 The record of the disclosure is reported verbally as soon as practicable to the Designated Safeguarding Lead (DSL) Andrew Kettle on 0203 515 8880 or 07823 321 993.

7.4 The staff member must submit a written record of the disclosure on a Student Incident Record Form (Head Office staff) or an email to Andrew Kettle andrew@academic-guardians.co.uk.

7.5 The DSL will hold an emergency strategy meeting to discuss the incident, assess the alleged threat and risk to the child (including any relevant facts about the child which may affect their vulnerability including age and ability), implement an action plan and continue to review the situation until a resolution has been achieved.

7.6 The meeting will be recorded with timed and dated entries within a Student Record – Incident Record to record all actions and updates.

7.7 The DSL will arrange for the young person to be helped and supported in recognition of the pressures they may have been under when using social networking sites; helping them to understand the wider issues and motivations, and making available information and material on the issues of consent, trust within healthy relationships and recognising abusive and coercive language and behaviors. This help and support could be provided from accredited organisations such as the school, Nation Society for the Prevention of Cruelty to Children (NSPCC), ChildLine and National Crime Agency (NCA) – Child Exploitation and Online Protection Centre (CEOP) websites and helplines.

7.8 The DSL will ensure that any viewing of images is only made where there are good and clear reasons to do so (unless unavoidable because the student has willingly shown a member of staff), basing incident decisions on what the DSL has been told about the content of the imagery. The DSL will ensure that staff members do not search through devices and delete imagery unless there is a good and clear reason to do so.

7.9 The DSL will consider the need to ask for the student to produce a device as evidence. The viewing of any images or seizing of any devices will be recorded including those present, date and time to meet Academic Guardians UK standards set out for recording incidents.

7.10 The DSL will consider the need to contact another school, college, setting or individual and whether to contact the parents or carers of the children involved. In most cases parents should be involved unless there is good reason to believe that involving these parties would put the young person at risk of harm.

7.11 The incident will be referred to a statutory agency (Children's Services on the Local Authority telephone number or the police by dialing 101) immediately if there is a concern a young person has been harmed or is at risk of harm. This would include information coming to light if at the initial stage:

- The incident involves an adult
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
- What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- The imagery involves sexual acts and any pupil in the imagery is under 13
- You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

7.12 If none of the above apply, the DSL may decide (with input from key stakeholders if appropriate) to respond to the incident without involving the police or children's social care (the DSL can choose to escalate the incident at any time if further information/concerns come to light). The decision should be recorded in line with the Safeguarding Policy and Child Protection Policy, and regularly reviewed throughout the process of responding to the incident.

7.13 The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved, and the risks can be managed within Academic Guardians UK support framework and network for the child.

7.14 The DSL will advise to the young person to delete imagery and to confirm they have deleted the imagery. Young people should be given a deadline for deletion across all devices, online storage or social media sites on the basis that possession of youth produced sexual imagery is illegal. Where a young person refuses or is later discovered to have not deleted the images, they are committing a criminal offence and the police may become involved. A record will be made of these decisions as per the Safeguarding Policy including decisions, times, dates and reasons. Academic Guardians UK may wish to invoke their own measures to discourage young people sharing, creating or receiving images in line with behavior policies.

7.15 Where the DSL is aware that youth produced sexual imagery has been unavoidably viewed by a member of staff, the DSL should ensure that the staff member has appropriate support. Viewing youth produced sexual imagery can be distressing for both young people and adults and appropriate emotional support may be required.

8 Additional Advice

8.1 Academic Guardians UK are aware of additional advice and support being offered from the following organisations:

Internet Watch Foundation

If a site has no reporting function and if the content is a sexual image of someone under 18 you can report it to the Internet Watch Foundation (IWF). Sexual images of anyone under 18 are illegal and the IWF can work to get them removed from sites which do not have reporting procedures. Adults can report directly to the IWF here: www.iwf.org.uk. Young people can contact ChildLine who work in partnership with the IWF and will support young people through the process.

NCA-CEOP

Parent Info from CEOP and Parent Zone -
http://parentinfo.org/article/online-teen-speak-updated
a guide to the most commonly used teen speak, slang words and acronyms to assist parents in understanding what their children are saying.

www.ceop.police.uk/safety-centre If you are concerned that a child is being sexually abused, exploited or groomed online you should report to NCA-CEOP

The Professionals Online Safety Helpline (POSH)

http://www.saferinternet.org.uk/about/helpline Tel: 0844 381 4772
The POSH helpline supports professionals with an online safety concern or an online safetyconcern for children in their care. Professionals can contact the helpline to resolve issues

Bullying UK

Bullying UK if you think you are being bullied call 0808 800 2222 or visit their website at – http://www.bullying.co.uk

Kidscape

There to provide children, families, carers and professionals with advice, training and practical tools to prevent bullying and protect young lives.
http://www.kidscape.org.uk