E-Safety Policy

2019

1. Introduction

1.1 It is the duty of the School to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, minors are accessing material through the internet which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

1.2 ICT in the 21st Century has an all-encompassing role within the lives of minors and adults. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by minors include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

1.3 The widespread use of digital communications technologies, as listed above, presents young people with a lot of opportunities for learning, participation, creativity and self-expression. At the same time, it poses a range of safeguarding concerns, which can be grouped as follows:

- **Content-** Student exposure to illegal, inappropriate or harmful online content including spam, pornography, substance abuse, violence, cyber-bullying, extremism and hate sites, and lifestyle sites that promote anorexia, self-harm or suicide.
- **Contact-** Students participate in exploitative digital communication including viruses and malware, personal data or identity theft, cyber-stalking, online grooming, anonymous online chat sites and cyber-bullying.
- **Conduct-** Concerns for students' health and well-being, such as gaming, gambling or social network addiction; online disclosure of personal information and ignorance of privacy settings; online reputation and 'sexting' (sending and receiving personally intimate digital images); and illegal conduct, including hacking, plagiarism, and copyright infringement of digital media, such as music and film.

1.4 E-safety is a shared responsibility; all staff, students and host families are encouraged to work together to develop strategies to promote a safe environment. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' understanding the risks to which that they may see, so that they have the confidence and skills to face and deal with these risks.

2. Purpose

2.1 The requirement to ensure that minors and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in young learner centres are bound. The purpose of the e-safety policy is to help to ensure safe and appropriate use. Junior centres aim to adopt the highest possible standards and to take all reasonable steps in relation to the safety and welfare of all students.

2.2 This Policy is based on and incorporates elements of the following legislation and national guidance documents (including but not limited to):

2.2.1 Racial and Religious Hatred Act 2016

2.2.2 Counter-Terrorism & Security Bill 2015

2.2.3 Criminal Justice Act 2003

2.2.4 Sexual Offences Act 2003

2.2.5 Communications Act 2003

2.2.6 Data Protection Act 2018

2.2.7 The Computer Misuse Act 1990

2.2.8 Malicious Communications Act 1998

2.2.9 Public Order Act 1986

2.2.10 Obscene Publications Act 1959 & 1964

2.2.11 Protection from Harassment Act 1997

2.2.12 Criminal Justice and Immigration Act 2008

2.2.13 Education and Inspections Act 2006

3. Scope

3.1 This E-safety policy together with the Social Media Policy applies to everyone working at or attending PLUS Junior Centres. It provides responsibilities on all staff, students, agency staff and volunteers, contractors, visitors and consultants. It shares the use of technology both on and off the campus premises and where there is a risk to the safety of students.

4. Policy Statement

4.1 The aim of the E-Safety policy is to create and maintain a safe, healthy and supportive learning and working environment for our students, staff and visitors alike. The aims of this policy are:

• to encourage students to make good use of the education opportunities presented by access to the internet and other electronic communication;
• to safeguard and promote the welfare of students by preventing cyber-bullying and other forms of abuse;
• to ensure students use technology safely and securely;
• to help students take responsibility for their own e-safety; and

4.2 PLUS Junior Centres will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a campus computer. PLUS cannot accept liability for the material accessed, or any consequences resulting from Internet use.

4.3 The use of computer systems without permission or for inappropriate purposes could mean that a criminal offence is committed under the Computer Misuse Act 1990 and breaches will be reported to the Police.

4.4 Methods to identify, assess and minimise risks will be reviewed regularly.

4.5 Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. Personal Data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

5. Responsibilities

5.1 Senior Management Team

The Senior Management Teams have a legal responsibility under the Prevent duty to make sure that this policy is implemented across PLUS Junior Centres. In addition, the Senior Management Team must ensure the following:

- To ensure that the centres follow all current e-safety advice to keep students and staff safe.
- To take the overall responsibility for the e-safety provision.
- To take overall responsibility for data and data security.
- To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant.
- To make sure there is training and advice for all staff.
- To liaise with the Local Authority and other relevant agencies where required.
- To delegate the day to day management of e-safety to the Campus Manager.

5.2 Safeguarding Panel / Campus Manager

- The Campus Manager will take day to day responsibility for e-safety issues. The Safeguarding Panel based in PLUS' head office has a leading role in establishing and reviewing the company's e-safety policies / documents.
- To promote an awareness and commitment to e-safeguarding throughout the centres.
- To liaise with ICT technical staff at the various centres.
- To help and provide training and advice for all staff.
- To remain regularly updated on e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from: sharing of personal data; access to illegal/inappropriate materials, inappropriate on-line contact with adults/strangers; potential or actual incidents of grooming; cyber bullying and use of social media.

5.3 Teaching & Leisure Staff

All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school's e-safety and acceptable usage policies
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, Students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

5.4 Students

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- To know and understand PLUS' policy on the taking / use of images and on cyber-bullying.

- Should understand the importance of good e-safety practice when using digital technologies out of school and realise that PLUS' e-safety policy also covers their actions out of school.
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

6. Internet

6.1 The campus' used by PLUS provide internet access to students to support its academic activities and the educational opportunities presented by such access.

7. Reporting incidents & Procedure

7.1 E-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers play a very important role; their observation of behaviour is essential in recognising concerns about Students and in developing trust so that issues are reported.

7.2 Students should report to the Campus Safeguarding Lead (CSL) if: they are troubled by something they have been exposed to on the internet; or they have evidence of an incident of wrong doing by another user, either on the campus network or outside it, where the behaviour could threaten someone's safety or welfare.

7.3 Similarly, staff and host families should report their concerns to the CSL, who will respond following procedures within the relevant company Safeguarding and Child Protection policy, for Bullying/Cyber-Bullying, and for Promoting Good Behaviour. Staff should also consider the Whistleblowing policy for procedures on how to report within the organisation.

7.4 Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the school will determine the level of response necessary for the offence disclosed. Following disclosure of this information this will need to be immediately reported to the Senior Management Team by the Campus Manager/Safeguarding Lead. The decision to involve Police will be made by the Senior Management Team and will be made as soon as possible, after contacting the Children Safeguarding Team or e-Safety officer, if the offence is deemed to be out of the remit of the company to deal with.

7.4.1 All members of the school community will be informed about the procedure for reporting e-Safety concerns.

7.4.2 The Safeguarding Panel based in PLUS' head office will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

7.4.3 The school will manage e-Safety incidents in accordance with PLUS' behaviour policy where appropriate.

7.4.4 PLUS will inform group leaders/agents/parents/carers/host families of any concern as and when required.

7.4.5 After any investigations are completed, the company will go through the facts, identify lessons learnt and implement any changes required.

7.4.6 Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Campus Manager will contact the Senior Management team and who will then inform the Police of the concern if required.

8. Staff Training

8.1 All new staff will be provided with information and guidance on e-safety matters to ensure awareness of current issues and to promote best practice**.** Detailed advice is also contained in the Staff Code of Conduct. Training is also provided to ensure staff know how to send or receive sensitive and personal data and understand the requirement to make sure there are passwords where the sensitivity requires data protection.

8.2 The following websites are recommended as further general guidance concerning e-safety: http://www.thinkuknow.co.uk/ and https://www.getsafeonline.org/

9. Management of Social Media & Social Networking

9.1 All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

9.2 Students will be reminded about the ease of uploading personal information, the associated dangers and the difficulty of removing an in appropriate image or information once published.

9.2.1 Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

9.2.2 Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

9.2.3 All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or may offend another individual.

9.2.4 Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour as outlined in the Staff Code of Conduct.

10. Cyber Bullying

10.1 Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" - DCSF 2007

10.2 Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When minors are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyber bullying and its effects.

10.3 A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers/ host families understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and try to stop this from happening. Promoting a culture of confident users will support innovation and safety.

10.4 There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- *Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst Students. These measures should be part of the school's behaviour policy which must be communicated to all Students, school staff and parents.*

10.5 Where bullying outside school (such as online or via text) is reported to a member of PLUS staff, it should be investigated and acted on. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind

that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If a member of PLUS staff feels that an offence may have been committed, they should seek assistance from the Campus Manager who will, in turn, inform the senior management team in head office.

10.5.1 Cyber bullying (along with all other forms of bullying) of any member of the campus community will not be tolerated.

10.5.2 All incidents of cyber bullying reported to PLUS will be recorded.

10.5.3 Students, staff and host families will be advised to keep a record of the bullying as evidence.

10.5.4 PLUS will take steps to identify the bully, where possible and appropriate. This may include identifying and interviewing possible witnesses and contacting the service provider and the police, if necessary.

10.5.5 Students, staff and host families will be required to work with PLUS to support the approach to cyber bullying and PLUS' e-Safety ethos.

Sanctions for those involved in cyber bullying may include:

- The bully will be asked to remove any material that is to be inappropriate or offensive
- An internet service provider or host may be contacted to remove content if the bully refuses or is unable to delete content.
- Other sanctions for Students and staff may also be used in accordance with PLUS' Anti-Bullying, Behaviour and Safeguarding Policies.
- Agents/parents/ host families of Students will be informed.
- The Police will be contacted by the Senior Management team if a criminal offence is suspected.

11. Revenge Pornography

11.1 Sharing private material as "revenge porn" online is illegal in England and Wales. The legislation, which went through Parliament as an amendment to the Criminal Justice and Courts Bill, came into force on Monday April 13th 2015. Clause 33 in the legislation defines Revenge pornography is the publication of explicit material portraying someone who has not allowed the image or video to be shared. The law now makes it illegal to disclose a "*private sexual photograph or film*" without the consent of the person in the content, and with the *intent to cause them distress*. It is not an offence under this section for the person to show the photograph or film to the individual.

11.2 Where illegal activity has taken place or is taking place involving students PLUS will determine the level of response necessary for the offence disclosed. Following disclosure of this information this will need to be immediately reported to the Senior Management Team by the Campus Manager. The decision to notify the Police will be made by the Senior Management Team and will be made immediately if deemed necessary.

12. Radicalisation & Extremism

12.1 PLUS Junior centres are subject to a duty under the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "*due regard to the need to prevent people from being drawn into terrorism*". This duty is known as the Prevent duty. Whilst this is a standalone policy, it is integral to our Prevent policy and should be applied as an extension to PLUS' current and established policies and procedures that cover this area.

12.2 If staff do become aware of or see signs of conflict, aggressive or extreme behaviour or opinions held by a student or group of students consult with the Campus Manager who will immediately refer to PLUS' Prevent lead and Senior Management team to decide a course of action.

12.3 Students may become susceptible to radicalisation through a range of social, personal and environmental factors. All students are provided with information and reminded of the prevent duty as part of their induction.

12.4 All users are reminded that they cannot access or otherwise interact with the internet and Social media which promotes, encourages or supports extremism, radicalisation and or facilitates terrorism on campus IT equipment or on personal devices.

12.5 PLUS Centres expect students not to use their personal devices outside School hours to access material that promotes, encourages or supports extremism, radicalisation and or facilitates terrorism.

13. Monitoring & Review

13.1 PLUS' Safeguarding Panel and Senior Management Team are responsible for reviewing this e-safety policy, in light of any incidents that have occurred, new technologies, in accordance with government guidance.

12. Further Information

The E-safety Policy should be read in conjunction with the following company policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Whistleblowing Policy
- Prevent Policy

Appendix 1

E Safety Record of Concern

Name of Child	
DOB	
Date of incident/ Disclosure **Time**	
Record any Disclosure from Child using their Words. Use: **Tell** **Explain** **Describe** **Outline** **To clarify/ gather information**	**Who?** **What?** **Where?** **When?**
What are your concerns with the Child?	
Detail anything you have observed and when.	

What Category does the disclosure best fit?	**Grooming**			
	Cyber bullying			
	Misuse of Social Networking Site			
	Sexting			
	Gaming			
	Underage Films			
	Misuse of Digital Camera			
	Other Please specify			
Any other information to consider				
Name (PRINT)		**Date**		
Position		**Signature**		