ARMY INSTITUTE OF EDUCATION (AIE)

BEING SAFE ONLINE PROTECTION AND SAFEGUARDING POLICY

(All are requested to download it, confirm having read it and abide by it)

1. **General**.

In view of the Internet and Social Media as the basic building block of Online Teaching-Learning process, it is essential that an Institute Level Online Conduct and Safety Policy is laid down for strict compliance by the Student-Teachers, Teachers and Non-Teaching Staff. Army Institute of Education (AIE) is committed to promoting and safeguarding the welfare of all Student-Teachers and an effective online safety strategy is paramount to this. This is particularly important with regard to the Prevent strategy, as a large portion of cases of misconduct and virtual crime happen through the online medium.

2. **Aim.**

The Aim of the AIE's online safety strategy is threefold:

2.1 To protect the whole AIE community from illegal, inappropriate and harmful content or contact;

2.2 To educate the whole AIE community about their access to and use of technology; and

2.3 To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

3. In considering the scope of the AIE's online safety strategy, the AIE will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as Technology).

4. This policy applies to all members of the AIE community, including staff and volunteers, Student-Teachers, parents/guardians and visitors, who have access to the AIE's Technology whether on or off AIE premises, or otherwise use Technology in a way which affects the welfare of other Student-Teachers or any member of the AIE community or where the culture or reputation of the AIE is put at risk.

5. The following policies, procedures and resource materials are also relevant to the AIE's online safety practices included hereafter:

5.1 Acceptable Use Policy for Student-Teachers

5.2 Safeguarding and Student-Teachers Protection

5.3 Anti-Bullying Measures

5.4 Risk Assessment Policy for Student-Teacher's Welfare

5.5 Staff Code of Conduct

5.6 Privacy Notice

6. These policies, procedures and resource materials are available to staff on the AIE Website and all are requested to download it, confirm having read, and abide by it.

Army Institute of Education
Greater Noida
★

7. **Principal and Designated Mentors (DMs).**

7.1 The Principal has overall executive responsibility for the safety and welfare of members of the AIE community. Registrar & HoA will assist her where matters escalate to levels of Disciplinary Committee/Proctorial Board.

7.2 The Designated Mentors are Teachers with lead responsibility for safeguarding and Student-Teachers protection. The responsibility of the DMs includes managing and safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the Being Safe Online Protection and Safeguarding Policy.

7.3 The DMs will work with the ICT In-charge and the IT Manager in monitoring Technology uses and practices across the AIE and assessing whether any improvements can be made to ensure the online safety and well-being of Student-Teachers.

7.4 The DMs will regularly monitor the Technology Incident Log maintained by the IT Manager.

7.5 The DMs will regularly update other Teachers/Non-Teaching Staff on the operation of the AIE's safeguarding arrangements, including online safety practices and procedures.

8. **IT Manager.**

8.1 The IT Manager, together with his team, is responsible for the effective operation of the AIE's filtering system so that Student-Teachers and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the AIE's network.

8.2 The IT Manager is responsible for ensuring that:

8.2.1 The AIE's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

8.2.3 The user may only use the AIE's Technology if they are properly authenticated and authorised;

8.2.4 The AIE has an effective filtering policy in place and that it is applied and updated on a regular basis;

8.2.4 The risks of Student-Teachers and staff circumventing the safeguards put in place by the AIE are minimised;

8.2.5 The use of the AIE's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation;

8.2.6 Monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the AIE's network and maintain logs of such usage.

8.3 The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the AIE to safeguarding issues.

8.4 The IT Manager will report regularly to the Principal on the operation of the AIE's Technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the AIE, s/he will escalate those concerns promptly to the appropriate DMs of the AIE.

8.5 The IT Manager is responsible for maintaining the Technology Incident Log and bringing any matters of safeguarding concern to the attention of the DMs in accordance with the AIE's Being Safe Online Protection and Safeguarding Policy and Procedures.

9. **All Staff.**

9.1 The AIE staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the AIE's policies and of safe practice with the Student-Teachers.

9.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in paragraph 5 above.

9.3 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the AIE's Being Safe Online Protection & Safeguarding Policy and Procedures.

10. **Parents & Guardians.**

10.1 The role of parents/guardians in ensuring that Student-Teachers understand how to stay safe when using Technology is crucial. The AIE expects parents to promote safe practice when using Technology and to:

10.1.1 Support the AIE in the implementation of this policy and report any concerns in line with the AIE's policies and procedures;

10.1.2 Talk to their ward to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

10.1.3 Encourage their ward to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another Student-Teacher or need support.

10.2 If parents have any concerns or require any information about online safety, they should contact the respective DMs.

11. **Student-Teachers**.

10.1 The safe use of Technology is integral to the AIE's ICT curriculum. Student-Teachers are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices.

10.2 Technology is included in the educational programmes followed in the AIE in the following ways:

10.2.1 Student-Teachers are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

10.2.2 Student-Teachers are enabled to explore and work with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

Army Institute of Education
Greater Noida

10.2.3 Student-Teachers are guided to recognise that a range of technology is used in places such as homes and AIE and encouraged to select and use appropriate technology for particular purpose(s).

10.3 The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial activities, teaching Student-Teachers:

10.3.1 About the risks associated with using the Technology and how to protect themselves and their peers from potential risks;

10.3.2 To be critically aware of content they access online and guided to validate accuracy of information;

10.2.4 How to recognise suspicious, bullying, radicalisation and extremist behaviour;

10.2.4 The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

10.2.5 The consequences of negative online behaviour; and

10.2.6 Tow to report cyberbullying and/or incidents that make Student-Teachers feel uncomfortable, embarrassed or and under threat and how the AIE will deal with those who behave badly/offensively.

10.4 **AIE's Acceptable Use of ICT Policy** for Student-Teachers sets out the AIE rules about the use of Technology including internet, email, social media and mobile electronic devices, helping Student-Teachers to protect themselves and others when using Technology. Student-Teachers are required to be reminded of the importance of this policy on a regular basis by DMs.

10.5 **Not everything online is trustworthy.**

10.5.1 Recognize the importance of assessing the reliability of a website

10.5.2 Evaluate the reliability and accuracy of online sources of information

10.5.3 Other content (such as blogs, online adverts and search results)

10.5.4 Contact (how others online may attempt to persuade us to follow a link, download a file or engage in other behavior).

10.6 **Securing oneself online through responsible use and self-regulation.** Read the terms and conditions for the use of social media platforms. Do note that you are giving a lot of your personal data when you sign up. Small print often contains hidden clauses waiving privacy rights and allowing the posted content to be sold on.

10.7 **Safe use of technology can be empowering.**

10.7.1 Do not be a bully.

10.7.2 Do not remain a bystander if you encounter online abuse and exploitation. Here is what you should do:

- Do not respond or retaliate. Be civil.
- Save the evidence. Take "Screen Shots" using the Snipping Tool in Windows. The mobiles also have a feature to take screen shots.
- Talk to a trusted adult or report to authorities and seek help.

- Block people who bully or make you uncomfortable or who you do not know. All social media platforms have a feature that allows you to block.

10.7.3 Prevent malicious or undesirable contacts through use of:-

- Preferences
- Privacy tools
- Pop-up blocker

10.7.4 Good practices to protect accounts and enhance online security:

- Select unique and strong passwords that are difficult to guess
- Do not share passwords
- Learn to block
- Control access
- Install firewall
- Use updated anti-virus software
- Use filtering software
- Use privacy settings and sharing controls

10.7.5 Measures to take before giving away or selling off old mobiles and computers:

- If you wish to transfer information from the old device to your new phone, simply do so before clearing the old one.
- Remove your information from the device you wish to dispose-off as phones tend to allow access to sensitive, personal information by performing a factory reset.
- Removing the SIM and SD cards as these cards also store personal information that a factory reset will not erase. You may also wish to keep your SIM card so that you can retain your old phone number by having the card transferred into your new device.
- Once your phone has been rid of personal information, you may now safely dispose of it.

10.8 **Legal implications of certain online action and content.**

Most users neither know nor understand the impact or the possible consequences of some of their online activities. Teaching them ethical and moral behavior in general, and an awareness of Student-Teachers/Individual rights can create empathy for the victims of their communication and may address some problems such as cyberbullying, humiliating comments. However, they also need to be made aware about the legal implications of some of their online actions. Please refer **Annexure 1** for details.

11. **Procedures for dealing with incidents of misuse.**

11.1 Staff, Student-Teachers and parents/ guardians are required to report incidents of misuse or suspected misuse to the AIE in accordance with this policy and the AIE's safeguarding and disciplinary policies and procedures.

11.2 **Misuse by Student-Teachers**.

11.2.1 Anyone who has any concern about the misuse of Technology by Student-Teachers should report it so that it can be dealt with in accordance with the AIE's behaviour and discipline policies, where there is an allegation of cyberbullying.

11.2.2 Anyone who has any concern about the welfare and safety of a peer/pupil must report it immediately in accordance with the AIE's online protection police & procedures.

11.3 **Misuse by Staff.**

11.3.1 Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the AIE's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

11.3.2 If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the Being Safe Online Protection & Safeguarding Policy and Procedures.

11.3.3 Registrar & HOA will be the Nodal Authority for dealing with Staff violations.

11.4 **Misuse by any user.**

5.4.1 Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the In-charge ICT or the Principal AIE.

5.4.2 The AIE reserves the right to withdraw access to the AIE's network by any user at any time and to report suspected illegal activity to the police.

5.4.3 If the AIE considers that any person is vulnerable to online abuse/crime the AIE will refer this to the police.

Date: 27 Jul 2022

Place : AIE Greater NOIDA

Army Institute of Education
Greater Noida
★

Abhilasha Gautam

(Dr Abhilasha Gautam)
Principal