PLUME
Maldon's Community Academy

E-Safety Policy

This policy has been approved by the Board of Trustees with reference to the academy's Equality Policy. The aims of the Equality Policy are to ensure that Plume Academy meets the needs of all, taking account of gender identity, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this academy we meet the diverse needs of students to ensure inclusion for all and that all students are prepared for full participation in a multi-ethnic society.

Last Reviewed: November 2022

Next Review: November 2023

Ratified: December 2022

Contents Page

E-Safety

Aims

Our academy aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

What is E– Safety?

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Roles and responsibilities

The Trustees

The Trustees have overall responsibility for monitoring this policy and holding the Executive Principal to account for its implementation.

The Trustee's will co-ordinate regular meetings with appropriate staff to discuss online safety, and behaviour logs that show online safety as provided by the designated safeguarding lead (DSL).

All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Executive Principal

The Executive Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in the academy, in particular:

- Supporting the Executive Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Executive Principal, Director of ICT Systems and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are put on SIMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in academy to the Executive Principal and/or Trustees

This list is not intended to be exhaustive.

The Director of ICT Systems

The Director of ICT Systems is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at the academy, including terrorist and extremist material
- Ensuring that the academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents and Carers

Parents and Carers are expected to:

- Notify a member of staff or the Executive Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents and carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

E-Safety and the role of the stakeholders:

'It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app'

Department for Education (2019)

E-Safety is the protection of individuals against the misuse of technology in various forms. In the current educational climate, ICT aids the development of the students of our academy. ICT formulates key areas of academy life for our students such as accessing school work via platforms such as Teams, researching for work, accessing homework via 'Satchel One', taking pictures for projects etc. Therefore, it is important that all stakeholders are aware of the dangers and detrimental impact misuse can have upon all involved and how to prevent bullying issues occurring via the misuse of technology and social media.

How does E-Safety link to bullying?

Cyberbullying is a common term used to describe the misuse of technology and social media to bully another person. There are many different forms of cyberbullying including:

- harassment - the act of sending offensive, rude or insulting messages and being abusive
- defamation - when someone sends information to another person about someone else that is untrue
- flaming - the use of extreme and offensive language to provoke a reaction from another person
- impersonation - hacking another person's account or creating an account as someone else
- outing and trickery - sharing of personal information about another person to reveal secrets
- cyberstalking - the act of sending and repeatedly sending texts, emails and messages to cause harassment
- exclusion - intentionally leaving someone out of a group whether it be chatting, gaming, Apps etc.

As an academy, we can ensure that all stakeholders are educated as to what constitutes cyberbullying and how the use of technology can be controlled through a positive and clear infrastructure. Therefore, reducing the number of incidents of cyberbullying and ensuring that we have a strong E-Safety ethos to support our Anti-Bullying Policy at Plume Academy.

E-Safety and the Role of all Stakeholders

*'The internet is essential to our education and learning experience. ICT forms a large part of our education and it is about being responsible when using the internet, technology or any form of social media.***'**

Plume, Maldon's Community Academy's Executive Student Council Representative (2022)

There are a number of actions that link to the term 'cyberbullying' and that is what as a group of stakeholders we must attempt to prevent before it occurs. Our Executive Student Council representatives have devised a 'do's and don'ts' list for all stakeholders in an attempt to assist, overcome and prevent any such action linked to cyberbullying arising.

Educating Parents and Carers about Online Safety

The school will raise parents and carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via the website.

The school will let parents and carers know:

- What systems the academy uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the academy (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Designated Safeguarding Lead, Mr Stoneman.

Concerns or queries about this policy can be raised with Mr Stoneman.

Training Staff

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, newsletters, briefings and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and the safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection policy.

Links with other policies

This e-safety policy is linked to our:

- Child protection policy
- Behaviour policy
- GDPR Policy
- Complaints Policy

The Do's and Don'ts: of E-Safety to Prevent Cyberbullying

Plume, Maldon's Community Academy		Parents/Carers		Students	
✓	✗	✓	✗	✓	✗
Deliver case studies within Personal Development (PD) lessons that provide relevant information for E-Safety	Do not allow access to restricted websites or technology that may hinder the safety of students	To apply filters and security measures in line with their provider to ensure child protection and E-Safety	Do not allow your son/daughter to access websites that are inappropriate for their age	Students to use technology sensibly and ensure they protect themselves	Do not access other people's accounts for social media websites
College students provide information to younger students of their experiences	Do not refrain from reporting all incidents of misuse to AHoYs - any information is key to investigations	Parental viewing should be applied to ensure students are not accessing inappropriate websites	Do not leave students of a certain age with the access to your technology if not monitored	Students to apply a degree of awareness - if 'something does not feel right do not participate'	Do not send explicit or inappropriate messages to anyone in any form
Protection and internet security to be embedded across all use of PCs within the academy	Do not allow access to censored or explicit viewing videos or music sites to any student of Plume	Monitor age restrictions on technology and social media to enhance safety of their son/daughter	Do not allow students to talk or meet with any person's unknown that have been met online	Must abide by the age restrictions of the social media websites to ensure safety	Do not hand out your password or passcode to access any technology or social media websites to others
De-briefs given to parents and carers to aid the stakeholders understanding of E-Safety	Do not attempt to update all internet security to prevent students accessing new technology	Access to certain technology should be limited if they believe it is a risk to their son/daughter	Do not allow access to the internet without sufficient internet security and filters in place	Responsibility is upon the students to only access social media accounts that are their own	Do not impersonate or try to replicate another person other than yourself
E-Safety contracts introduced across ICT lessons to ensure students sign an agreement for their use of computers and technology within the academy	Do not withhold information regarding potential new dangers regarding technology and E-Safety to all stakeholders of Plume Academy	Ensure that as parents/carers you keep to up to date with any changes or developments in technology where your son/daughter may be impacted	Do not allow any information to be deleted in regard to cyberbullying and ensure complete transparency with regard to reporting it to the academy	Treat others on social media and via technology with the respect that you wish to be shown yourself	The internet and technology should be inclusive and should not be used to target any individual or to attempt to leave them feeling excluded socially