Greek School *of* Ayia Triada Birmingham

e-Safety Policy

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and members of Management Board
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) 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.

The policy also takes into account the National Curriculum computing programmes of study.

3.E-Safety - Roles and Responsibilities

3.1. Management Board

The MB has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The MB will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Chair of MB who oversees online safety is the Chair of Governors, and the IT person of GSAT.

All Members of MB:

- 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

3.2. The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school’s DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions and takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the ICT as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged 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 school policies

- 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 school to the headteacher and/or governing board This list is not intended to be exhaustive.

3.4 The IT person

is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring 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 policies

This list is not intended to be exhaustive.

3.5 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

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher 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 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 – Child net International
- Parent factsheet – Child net International
- Healthy relationships – Disrespect Nobody

3.7 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.

3.8 Other

The school also has a Digital Leaders committee which links to the School Council

4. Developing Student Awareness

On an E-safety Awareness Day, we will ensure children are taught about:

- Using technology safely and respectfully, keeping personal information private
- Identifying where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

5. Staff e-Safety Skills Development Training

- 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, e-bulletins and staff meetings).
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

- The Headteacher/ Chair of MB 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.
- Members of MB 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 and safeguarding policy.

6. Managing the School e-safety Messages

- The e-safety policy will be introduced to the pupils at the beginning of each school year.
- E-safety posters will be prominently displayed in the IT suite.
- There is a dedicated e-safety page on the school website which provides information to parents and pupils, signposts for support, websites etc.

7. Incident Reporting, e-safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's e-safety coordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must also be reported to the GDPR coordinator who will report incidents to GDPR depending on the severity of the breach.

E-safety Incident Log

Any incident related to e-safety will be recorded and be dealt accordingly

- These could include accidental or unintentional access to unsuitable websites, Internet searches which bring up undesirable content or minor misuse IT.
- These should be recorded on the minor incident form in the IT suite and the e-safety coordinator made aware. The incidents will then be assessed in case further action is needed. Further Action or More Serious Incidents

8. Misuse and Infringements

8.1 Cyberbullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and the anti-bullying policy.)

8.2 Preventing and addressing cyber-bullying

E-safety practice is always advocated in school.
At GSAT the following will take place:

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.
- We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Information for parents will be put on newsletters and published in the school's website; a meeting for parents to discuss internet safety will be offered annually.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so. Whilst the school recognises that cyberbullying may take place out of school hours, it will wherever possible, step in to mediate a suitable solution.
- Additionally no mobile phones, smart devices are permitted within the school premises and at all times of school operation

8.3 Peer on Peer Abuse

This school recognises that children sometimes display harmful behaviour themselves and that such incidents or allegations must be referred on for appropriate support and intervention.

Such abuse is unacceptable and will not be tolerated.

In the context of this policy, this abuse could for example include:

- 'upskirting'
- all forms of bullying via electronic devices
- aggravated sexting

8.4 Electronic Devices

Electronic devices are not permitted to use within the school premises and all parents are made aware of this. Children are encouraged to surrender their electronic devices as soon as they enter school. Devices will then be stored securely up until the end of the day and then will be returned.

Also, School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules.
- If a device is found to be brought in school and in use during school hours will be taken and parents will be notified.

- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device • Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the IT Network Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures, staff code of conduct or social media policy]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every 2 years by the ICT lead in our school. At every review, the policy will be shared with the Management Board of GSAT

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy

- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Version Control

Version Name	**Date**	**Reason for Update**
Next Review	01/09/2021	First Introduced
Reviewed	20/09/2022	Reviewed and approved
Next Review	20/09/2024	