GESHER SCHOOL

ENGAGE EMPOWER EDUCATE

Online Safety Policy

Date	Review Date	Coordinator	Nominated Governor
March 2021	March 2022	Chris Gurney	Mark Cohen

Contents

1. Introduction

At Gesher School, we are committed to safeguarding and promoting the welfare of all pupils in our care. Our online strategy enables us to create a safe online learning environment that:

- Promotes the teaching of Computing within the curriculum
- Protects children from harm
- Safeguards staff in their contact with pupils and their own use of the Internet
- Ensures the school fulfils its duty of care to pupils
- Provides clear expectations for all on acceptable use of the Internet (please also see the Gesher Acceptable IT Use Policy).

We have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that used correctly, Internet access will not only raise standards, but it will support teachers' professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security, as and where appropriate and as part of a safe learning environment

Online safety, which encompasses Internet technologies as well as learning about and (where appropriate) using forms of electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all pupils and other members of the school community have an entitlement to safe and secure Internet access.

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremist groups who wish to radicalize vulnerable children and to involve them in terrorism or in activity that supports terrorism. School personnel must be aware of the increased risk of online radicalization, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that school personnel are able to identify those who may be vulnerable to radicalization or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote pupils' welfare. Within this environment we work hard to build pupils' resilience to radicalization and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want pupils to develop their knowledge and skills in order to challenge extremist views.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that are connected with this policy.

2. Aims

- To ensure that there is a secure firewall in place with regular monitoring of internet use by staff and children with immediate action take if inappropriate use is discovered i.e. referral to the DSL and to the LADO or Children's Services in the case of misuse by a child

- To provide pupils with quality, appropriate and monitored Internet access as part of their learning experience across all curricular areas

- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet

- To evaluate Internet information and to take care of their own safety and security

- To raise educational standards and promote pupil achievement

- To protect children from the risk of radicalization and extremism

- To ensure compliance with all relevant legislation connected to this policy

- To work with other schools and organizations to share good practice in order to improve this policy

- To establish clear mechanisms to identify, intervene and escalate any incidents where there is cause for concern

3. 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 Department'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.

4. Role and Responsibilities

The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body 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).

All governors 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

The Headteacher

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

The Designated Safeguarding Lead

Details of the school's DSL are set out in our child protection and safeguarding policy.

The DSL 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 headteacher, IT support team, and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged via CPOMS 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 Anti-Bullying 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 school to the headteacher and/or governing board

The IT Support Team

The IT support team 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
- Ensuring that the school'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 on a regular basis
- 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 anti-bullying policy with the support of the DSL/headteacher

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 anti-bullying policy

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child adheres 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 - Childnet International

- Parent factsheet - 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. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

6. Educating Parents About Online Safety

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

Where applicable, parents will be expected to complete online safety training that is provided by the school.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher/DSL.

7. Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and Addressing Cyber-Bullying

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. As a school with a highly vulnerable demographic, Gesher will strive to ensure there are accessible ways in which children can communicate their concerns.

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. Teacher will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying and safeguarding policies. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

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.

8. Acceptable Use Of The Internet In School

All pupils, parents, staff, volunteers and governors are expected to read the Gesher Acceptable Use of ICT Policy and sign the attached agreement. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Gesher will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Gesher Acceptable Use of ICT Policy.

9. Internet Filtering and Use

We shall be entering into a contract with a reputed and national Internet provider to manage a secure and filtered Internet service which enables us to safely access and use the Internet and all email. The Internet filtering service will be annually reviewed.

Access to the Internet is designed to protect pupils and school personnel by blocking the following content:

- adult content containing sexually explicit images
- violent content containing graphically violent images
- hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- illegal drug taking content relating to the use or promotion of illegal drugs or the misuse or prescription drugs
- criminal content relating to the promotion of criminal and other activities
- gambling content relating to the use of online gambling websites
- any inappropriate, non educational websites such as some social networking sites (some such sites may be made available if deemed to have educational value)

All users access the Internet in accordance with the School's Acceptable Internet Use & Agreement and will inform the ICT support team if at any time they find they have accessed inappropriate Internet sites.

When inappropriate material has been accessed the Internet Service Provider will be contacted and if necessary the Police.

10. Authorising Internet Access

- Before using any school ICT resource, all staff must read and sign the 'Acceptable IT Use Agreement'.

- Parents must sign a consent form before their child has access to the Internet.

- An up-to-date record will be kept of all pupils and school personnel who have Internet access.

11. Password Security

All users are responsible for the security of their username and password and must not allow other users to use this information to access the system. All breaches of security must be reported.

12. School Website

Contact details on the website are as follows:

- the school address

- the school e-mail address (including those of staff members)

- the school telephone number

- The school website will not publish:

- staff or pupils contact details

- the pictures of children without the written consent of the parent/carer

- the last names of any pupils who are shown

13. Social networking

Pupils will not be allowed access:

- to social networking sites except those that are part of an educational network or approved Learning Platform
- to newsgroups unless an identified need has been approved

14. Internet System Security

- New programs will be installed onto the network or stand-alone machines by the IT support team

- Everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence

15. Pupils Using Personal Electronic Devices In School

Children are discouraged from bringing electronic devices to school without written permission from the headteacher. A check list will be held by the school office and classroom teacher to ensure any permitted devices are collected upon arrival at school, where they will be held securely in the school office until the child leaves the school to go home (the school office will cross-reference this against the morning register to ensure this is actioned each day). The school will not be held liable for any damage that may occur to such devices whilst on school property.

Personal electronic devices are not to be accessed on-site. Any devices found to be held by a pupil on school premises will be viewed as a prohibited item and confiscated. Parents will be informed and follow-up actions may take place as per the Gesher Behaviour Policy.

Examining Electronic Devices

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
- Disrupt teaching
- Break any of the school rules

All efforts will be made by the school to contact parents/carers to notify them of any searches, but permission does not have to be given to proceed with this. Any inappropriate material found on electronic devices will be subject to the appropriate follow-up actions; these may include discussions with parents, indefinite removal of permissions to bring devices on site, or referrals to the Local Authority Safeguarding Team/police department.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure

Any electronic devices found on school property may be subject to a search by the Senior Leadership Team if they suspect the material on that phone may cause harm, breach school rules, or cause disruption to teaching.

16. Staff Using Work Devices Outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of Acceptable Use of ICT Policy.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT support team.

Work devices must be used solely for work activities, and all usage must be in line with the Gesher Remote Working Policy.

17. Complaints of Internet Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Anti-Bullying, Acceptable Use of ICT, and Child Protection & Safeguarding. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Parents will be informed of all such incidents.

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 and staff code of conduct. 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.

18. 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.

The DSL and deputies 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.

Governors 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 & Safeguarding Policy.

Monitoring

The policy will be reviewed annually by the policy coordinator.

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
- Acceptable use of ICT policy
- Remote working policy
- Anti-bullying policy

APPENDIX

Internet Permission Form

Please complete and return this form to the School as soon as possible.

As part of your child's study at school there will be times when s/he will need to gain access to the Internet. In order for your child to make use of the school's internet facilities we require that this form is completed and signed.

Pupil Name: _____________________________________

Class: ____

____
_____

Parent or Guardian

As the parent or legal guardian of the pupil named above, I grant permission for my son / daughter to the Internet in school. I understand that the school has taken reasonable care to protect its pupils from inappropriate and objectionable materials but that this protection cannot be guaranteed to be 100% successful. I also understand that pupils will be held accountable for their own actions. I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media.

Parent/Guardian's signature: ______________________________

Date: __________________