GESHER SCHOOL

ENGAGE EMPOWER EDUCATE

Acceptable Use of IT Policy

Date	Review Date	Coordinator	Nominated Governor
March 2021	March 2022	Tamaryn Yartu	Howard Zetter

Acceptable Use of IT

Gesher believe information and communications technology includes all forms of computing, the internet, telecommunications, digital media and mobile phones. School personnel have clear responsibilities with regard to the use of all IT equipment and IT facilities.

Gesher School and the Gesher Trust are committed to safeguarding and promoting the welfare of all pupils in our care. Our e-safety strategy enables us to create a safe e-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

Any member of the school personnel including staff (including temporary staff and contactors), governors and trustees that uses illegal software or access inappropriate websites when in school will be subject to disciplinary proceedings which may result in dismissal. All school personnel will be made aware of all legislation relating to computer misuse, data protection and copyright.

We require all school personnel to sign and date the 'Acceptable Use of IT Agreement' and be fully aware of and implement the internet safety policy. All school personnel have the duty to report any misuse of the IT equipment or the IT facilities of this school.

We have a duty to ensure the internet safety of all pupils within this school.

We have London Grid for learning filtering system to support this.

Aims

To ensure school personnel are aware of all legislation relating to computer misuse, data protection and copyright and implement this policy

- To share good practice within the school
- To protect children from the risk of online abuse and bullying including radicalisation and extremism
- To work with other schools and organisations in order to share good practice in order to improve this policy

Responsibility for the Policy and Procedure

Role of the Governing Body

The Governing Body has:

- Appointed a designated governor to be responsible for IT and E-Safety
- Delegated powers and responsibilities to the Headteacher to ensure all school personnel and stakeholders are aware of and comply with this policy
- Responsibility for ensuring full compliance with all statutory responsibilities
- Responsibility for ensuring that the school complies with all equalities legislation
- Nominated a designated Equalities governor to ensure that appropriate action will be taken to deal with all prejudice related incidents or incidents which are a breach of this policy
- Responsibility for ensuring funding is in place to support this policy
- Responsibility for ensuring this policy and all policies are maintained and updated regularly
- Responsibility for ensuring all policies are made available to parents
- Make effective use of relevant research and information to improve this policy
- Nominated a link governor to visit the school regularly, to liaise with the Headteacher and the coordinator and to report back to the Governing Body
- Responsibility for the effective implementation, monitoring and evaluation of this policy

Role of the Headteacher and Senior Leadership Team

The Headteacher and the Senior Leadership Team will:

- Ensure all school personnel are aware of and comply with this policy
- Ensure all school personnel sign and date the 'Acceptable Use of IT Agreement'
- Work closely with the link governor and coordinator
- Provide leadership and vision in respect of e-safety
- Provide guidance, support and training to all staff
- Make effective use of relevant research and information to improve this policy

- Monitor the effectiveness of this policy
- Annually report to the Governing Body on the success and development of this policy

Role of the IT Coordinator

The coordinator will:

- Lead the development of this policy throughout the school
- Work closely with the Headteacher and the nominated governor
- Devise and update when appropriate acceptable use guidelines
- Display these guidelines around the school
- Provide guidance and support to all staff
- Keep a log of all IT equipment used by school personnel
- Provide training for all staff on induction and when the need arises regarding
- Make effective use of relevant research and information to improve this policy
- Keep up to date with new developments and resources
- Undertake risk assessments when required
- Review and monitor use of IT equipment including reporting outcomes to the Headteacher and Governor responsible for e-safety
- Annually report to the Governing Body on the success and development of this policy

Role of the Nominated Governor

The Nominated Governor will:

- Work closely with the Headteacher and the IT Coordinator
- Ensure this policy and other linked policies are up to date
- Ensure that everyone connected with the school is aware of this policy
- Attend training related to this policy
- Report to the Governing Body every term
- Annually report to the Governing Body on the success and development of this policy including monitoring of IT use by pupils and staff

Role of School Personnel

School personnel will:

- Comply with all aspects of this policy
- Be aware of all other linked policies
- Sign and date the 'Acceptable Use of IT Agreement'
- Be aware of the acceptable use guidelines
- Protect their user name and passwords
- Log off when using a computer
- Implement the school's Equalities Policy and procedures
- Report and deal with all incidents of discrimination
- Attend appropriate training sessions on equality
- Report any concerns they have on any aspect of the school community

Teaching e-safety

One of the key features of our e-safety strategy is teaching pupils to protect themselves and behave responsibly while online. The Headteacher has overall responsibility for the coordination of e-safety education, but all teaching staff play a role in delivering e-safety messages in language which is appropriate to their age.

Pupils are taught:

- The benefits and risks of using the internet
- How their behaviour can put themselves and others at risk
- What strategies they can use to keep themselves safe
- How to build resilience to protect themselves and their peers
- What to do if concerned about something they've seen on the internet
- Who to contact with concerns
- That the school has a 'no blame' policy so pupils are encouraged to report any e-safety incidents

- The school has a 'no tolerance' policy regarding cyber bullying

- That behaviour that breaches acceptable use will be subject to sanctions and disciplinary action

In the event that a pupil accidentally accesses inappropriate materials they must report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action. Where a pupil feels unable to disclose abuse, sexual requests or other misuses against them to an adult they can use the Report Abuse button (www.thinkuknow.co.uk or ceop.police.uk) to make a report or seek further advice.

E-mails (as appropriate)

Children are taught about e-mail use as part of the Computing curriculum. The following areas are covered:

- Children are taught not to disclose personal contact details via e-mail correspondence

- All e-mail communications should be polite and if a pupil receives an offensive e-mail, they should not reply but tell a teacher immediately

- Children are made aware that by bullying via e-mail will not be tolerated and will be dealt with in accordance with the anti-bullying policy

- Users must be aware that use of e-mail is for educational purposes only and will be monitored

- Children must not open attachments if they are unsure of the content or have no knowledge of the sender

Acceptable use of social networking sites in school

The widespread availability and use of social networking bring opportunities to understand, engage and communicate with the outside world in new ways. It is important that pupils are able to use these technologies and services effectively and flexibly and in an age-appropriate way. However, it is also important to ensure that our legal responsibilities and our reputation are upheld to the highest standards. For example, use of social networking applications has implications for the duty to safeguard pupils.

Some examples of social networking applications are:

- Blogs

- Online discussion forums

- Collaborative spaces, Media sharing services e.g. Youtube
- 'Micro logging' applications e.g. Twitter

- Virtual worlds – MMORPG (Massive Multiplayer Online Role Playing Games – e.g. World of Warcraft, Runescape)

The use of social networking sites within schools is only allowed in appropriately controlled situations and in support of legitimate curriculum activities – for example to teach the safe use of the internet. All incidents of complaints relating to e-safety and unacceptable internet use must be reported to the Head or one of the Designated Safeguarding Leads (DSLs) immediately.

A log will be kept of all e-safety incidents and complaints to monitor emerging patterns of individual behaviour or weaknesses in the schools' systems. These records will be kept in the central 'Incidents File'.

If a pupil unintentionally opens a website with distressing or inappropriate content, teachers must immediately close the screen, reassure the pupil that they have done nothing wrong and report the details of the website to the Head or DSL who will then ensure that the site is blocked.

If a pupil intentionally accesses an inappropriate they will be subject to the sanctions set out in the Behaviour & Discipline Policy.

Cyber Bullying

Cyber bullying is defined as the use of technology to deliberately hurt or upset someone. The internet allows bullying to continue past school hours and invades the victim's home life and personal space and allows for hurtful comments and material to be available to a wider audience.

Bullying may take the form of:

- Rude, abusive or threatening messages via e-mail, text or social networking sites (as listed above)

- Posting insulting, derogatory or defamatory statement on blogs or social networking sites
- Setting up websites that specifically target a victim

- Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail. Cyber bullying can affect both pupils and staff and it could be deemed a criminal offence

- Incidents of cyber bullying will be reported to the Head or Assistant/Deputy Head and if extreme may in turn be reported to the police

- Pupils are taught to only give out mobile phone numbers an e-mail addresses to trusted people; not to respond to offensive messages and to report these immediately to an appropriate adult

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing and blocking communications and will give advice to parents and teachers. Parents must be notified of any such incidents so they can block any offensive messages on home computers.

Mobile Phones and Other Portable Electronic Devices

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.

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. All efforts will be made by the school to contact parents 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.

Working with Parents

Parents will be directly involved in the development and implementation of e-safety strategies and policies. On receipt of the school's E-safety policy, they will be asked to sign the 'Acceptable IT Use Agreement' in conjunction with their child. Information about e-safety will be shared with parents periodically and in a variety of different forms

Acceptable IT Use Agreement (Staff)

I understand that the school Internet facility is for the good of my professional development, for the development of this school and must be used only for educational purposes.

I realise that I have a personal responsibility to abide by the set rules and regulations when using the Internet. I am aware that the school monitor and filter internet use through London Grid for Learning (LGFL's) WebScreen filtering Service and I am additionally aware of the consequences if I breach them.

I am aware that by breaching the rules and regulations it may lead to:

- Withdrawal of my user access
- The monitoring of how I use the Internet
- Disciplinary action
- Criminal prosecution

I will report immediately to the E-Safety Coordinator any accidental access to inappropriate material or websites that I may have.

I will log on to the Internet by using my password, which will be changed every half term, or if I think someone knows it.

When using the school's Internet, I will not:

- Use the Internet in such a way that it will bring the school into disrepute
- Use inappropriate or illegal websites
- Download inappropriate material or unapproved software
- Disrupt the time of other Internet users by misusing the Internet
- Use inappropriate language
- Use language that may provoke hatred against any ethnic, religious or other minority group
- Produce, send out, exhibit or publish material that will cause offence to anyone
- Divulge any personal information about myself, any other user or that of pupils
- Divulge my login credentials or passwords to anyone
- Use the login credentials or passwords of any other user
- Use a computer that is logged on by another user
- Use any social networking site inappropriately but only to use it in order to develop teaching and learning
- Transfer the images of pupils without prior permission of the headteacher and from parents
- Use email for private use but only for educational purposes
- Compromise current data protection law or the law of copyright in any way

I agree to abide by this agreement:

Employee Name:		**Headteacher Name:**	
Employee Signature:		**Headteacher Signature:**	

Acceptable IT Use Policy for Children
(to be used where appropriate)

CHILD

I want to stay safe while I am using a computer and I know that anything I do on a computer can and may be seen by others.

I will:

- Keep my password a secret (but not from parents or teachers)
- Only open pages which my teacher has said are OK
- Tell my teacher or parent if anything makes me feel scared or uncomfortable
- Make sure all the messages I send are polite
- Tell my teacher or parent if a get a nasty message
- Not to reply to any nasty message which makes be feel upset or uncomfortable
- Not to give my mobile number, home address or address to anyone who is not a real friend – and not without the permission of my parents or teacher
- Only e-mail people I know or if my teacher or parent agrees
- Talk to my parents or teacher before using anything on the internet
- Not load any photographs of myself onto the computer
- Never agree to meet a stranger
- Leave any electronic devices with the school office upon arrival to school property

Signed _____ (by pupil) Date _____

PARENT

I have read the above school rules for responsible internet use. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.

Signed _____(by parent) Date _____

Raising Awareness of this Policy

We will raise awareness of this policy via:

- the Staff Handbook
- meetings with school personnel

Training

All school personnel:

- have equal chances of training, career development and promotion
- receive training on this policy on induction which specifically covers:
    - Computer Misuse
    - Data Protection
    - Copyright
    - Equal opportunities
    - Inclusion

- receive periodic training so that they are kept up to date with new information
- receive equal opportunities training on induction in order to improve their understanding of the Equality Act 2010 and its implications