THE GOWER SCHOOL

E – SAFETY POLICY

This policy applies to the whole school including the Early Years Foundation Stage (EYFS)

The Policy is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office. All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours including activities away from school.

Monitoring and Review: This policy is subject to continuous monitoring, refinement and audit by Emma Gowers (Principal, Proprietor and Designated Safeguarding Lead (DSL). The Proprietor will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. The Proprietor recognises that staff build expertise by undertaking safeguarding training and managing safeguarding concerns. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the update/reviewed policy and it is made available to them in either a hard copy or electronically.

Signed:

Emma Gowers

Miss Emma Gowers
Principal and Proprietor

Date reviewed: June 2022
Date of next review: June 2023

This policy was last reviewed by the Principal/Proprietor and Senior Leadership Team (SLT) in June 2022 and will next be reviewed no later than June 2023 or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Introduction: The primary purpose of this policy is to safeguard pupils and staff at The Gower School. It details the actions and behaviour required from pupils and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements we have a whole school approach to e-safety. Our key message to keep pupils and young people safe is to be promoted and will be applied to both online and offline behaviours. Within our E-Safety Policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding Policy.

This policy should be read alongside our organisational policies and procedures, including:

- Safeguarding policy, including Designated Safeguarding Leads
- dealing with allegations of abuse made against a child or young person
- managing allegations against staff and volunteers
- code of conduct for staff and volunteers
- anti-bullying policy and behaviour management procedures
- photography and image sharing guidance
- Preventing Extremism and Tackling Radicalisation Policy.
- The staff and pupil Acceptable Use Policies (AUPs)
- Spiritual, Moral, Social and Cultural Development and Personal, social, health and economic education

Legal Status:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Children Safe in Education* (September 2022)
- *Working Together to Safeguard Children A guide to inter-agency working to safeguard and promote the welfare of children (2018)*
- *Statutory guidance - Revised Prevent duty guidance: for England and Wales (Updated 1 April 2021)*
- *How social media is used to encourage travel to Syria and Iraq, briefing note for school (DfE 2015)*
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying' and Preventing and Tackling Bullying 2017
- Prepared with reference to DfE Guidance (2014) *Preventing and Tackling Bullying: Advice for school leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in schools.*
- The Data Protection Act 1998; BECTA (British Educational Communication and Technology Agency**)** and CEO(Child Exploitation and Online Protection Command)

The E-Safety Policy will be reviewed annually by the Principal/Proprietor and SLT who will provide recommendations for updating the policy in light of experience and changes in legislation or technologies. All staff should read these policies in conjunction with the E-Safety Policy. This is particularly important with regard to the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Safeguarding Policy and Preventing Extremism and Tackling Radicalisation Policies.

Roles and Responsibilities: Our nominated E-Safety Officer is Miss Emma Gowers (Principal/Proprietor) who has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice. This role overlaps with that of the Designated Safeguarding Lead (DSL) role in all matters regarding safeguarding and E-safety. The roles include ensuring:

- Young people know how to use the Internet responsibly and that parents and teachers have the right measures in place to keep pupils safe from exploitation or radicalisation.
- Pupils are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- To ensure that pupils use Information and Communications Technology (ICT) safely and securely and are aware of both external and peer to peer risks when using ICT, including cyberbullying and other forms of abuse.
- All staff, volunteers and the proprietor receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- The Acceptable Use Policy (AUP) is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be transparent and updated as agreed in school policies.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- An appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- A current record of all staff and pupils who are granted access to school ICT system is maintained.

Staff/Volunteers Use of IT Systems:

Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the 'Staff Code of Conduct for ICT) before using any school ICT resource. In addition:

- All staff will receive annual update e-safety training.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems will be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password protected computers and other devices. Staff are advised to follow the "How do I stay secure on the Internet?" section in the E-Safety FAQ document.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- Occasionally pupils may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study and monitor internet use closely. Every request to do so should be auditable with clear reasons for the need.
- The Internet can be used actively to gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved web browsers and email systems which have appropriate security in place. Additionally, files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes.
- Additionally, staff should not communicate with pupils through electronic methods such as social networking sites, blogging, chat rooms, texts or private email. Instead, only the school email system should be used for this purpose.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e. videos of lessons, activities or fieldtrips, should be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.

Any person suspecting another of deliberate misuse or abuse of technology must take the following action:

1. Report in confidence to the school's E-Safety Officer.
2. The E-Safety Officer should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the Child Exploitation and Online Protection Centre (CEOP) or the police will be informed.
5. No pupil or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

Systems and Access

Staff members are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school ICT equipment or their own PC

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or

disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Equality Act 2010)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998. Changes under the future UK-EU relationship to copyright law from January 1st 2021. Guidance can be found on https://www.gov.uk/guidance/changes-to-copyright-law
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment, they must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

Teaching and Learning: Internet use is part of the curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. E-safety is a focus in all areas of the curriculum and key e-safety messages are reinforced regularly, teaching pupils about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Staff should be vigilant in lessons where pupils use the Internet. Staff will be provided with sufficient e-safety training to protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety, together with specific safeguarding issues including cyberbullying/cybercrime and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school has a system for teaching internet skills in ICT lessons
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-Safety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are aware of the impact of Cyberbullying/cybercrime and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Cyber-mentors, Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

Pupils Use of IT Systems: Pupils at The Gower School will be given supervised access to our computing facilities and will be provided with access to filtered Internet and other services operating at the school. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of pupils and young people. The Gower School will help pupils to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, social, health and economic (PSHE) education and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)

Communicating and Educating Parents/Guardians in Online Safety: Parents will be provided with a copy of the IT User Acceptance Policy, and parents will be asked to sign it, as well as pupils in Key Stage 2. The Gower School recognises the crucial role that parents play in the protection of their pupils with regards to online safety. The school organises an annual awareness session for parents with regards to e-safety which looks at emerging technologies and the latest ways to safeguard pupils from inappropriate content. The school will also provide parents and carers with information through newsletters, web site and the parent portals. Parents and guardians are always welcome to discuss their concerns on e-safety with the school, who can direct them to the support of our E-Safety Officer if required. Parents and carers will be encouraged to support the school in promoting good e-safety practice.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to GDPR. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. The unauthorised access or use of personal information, contrary to the previsions of the Data Protection Act is not permitted. Virus protection will be updated regularly. If a 'virus alert' occurs when transferring work from one device to another a member of SLT staff must be informed immediately. All external hardware e.g. memory sticks must be vetted by submitting them to an anti-virus check.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff are not permitted to access their personal social media accounts using school equipment at any time whilst on duty
- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of social media
- Pupils should be reminded that the legal age to have a social media account is 13, and therefore no TGS student should have an account
- Staff, pupils are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, pupils, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, pupils are aware that their online behaviour should at all times be compatible with UK law.

Radicalisation and the Use of Social Media to Encourage Extremism: The Internet and the use of social media in particular has become a major way to communicate with others, which has provided access for like-minded people to create an online community and confirm extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people;
- Confirming extreme beliefs;
- Accessing likeminded people where they are not able to do this off-line, creating an online community;
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

The Gower School has a number of measures in place to help prevent the use of social media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils.
- Pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*

Reporting of E-Safety Issues and Concerns Including Concerns Regarding Radicalisation: The Gower School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding e-safety should be made to the DSLs, who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the DSLs. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Policy. Our DSLs provide advice and support to other members of staff on protecting pupils from the risk of on-line radicalisation. The Gower School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. Staff safeguard and promote the welfare of pupils and know where and how to refer pupils and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Emerging technologies, such as mobile phones with Internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.
- We will audit ICT use to establish if the E-Safety Policy is sufficiently robust and that the implementation of the E-Safety Policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The DSL will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered *Wi-Fi* access.
- The Gower School takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard pupils from potentially harmful and inappropriate material on-line without unreasonable "over-blocking" (para 133, KCSIE Sept 2022).
- The Gower School recognises that pupils may choose to circumvent certain safety precautions by using devices over 3G, 4G and 5G. To help provide a safe environment for all pupils, we will supplement the systems filtering with behaviour management and additional staff/pupil training.

Internet Security and Filtering Systems

The Gower School security has in place systems which monitor and secure the internet traffic at the school. These systems are to keep everyone safe, from blocking inappropriate content, to protecting our ICT systems from cyber-attacks. The monitoring side plays an important part of the system, which helps us to identify ways to improve security, and to better protect those that use it. By default, the system blocks all inappropriate websites, illegal or unsuitable content, including pornography. Use of these kinds of site is not allowed at the school.

E-mail Usage:

- Staff must not reply to or forward on an offensive e-mail and must immediately inform a member of SLT or a DSL.
- Personal e-mail or messaging between staff and pupils should not take place
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Staff must be vigilant for spam, phishing emails and scam emails which may contain viruses or ransomware and can attack our system, as per staff training on this.
- The forwarding of chain letters is not permitted.
- Staff may not correspond directly with parents using their school email address – this is for internal use only

Authorising Internet Access:

- All primary staff have training on the use of 'Purple Mash and Online Safety' and use this as the primary learning tool with the children.
- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- We will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Foundation Stage and Key Stage 1 and 2, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form for both internet use and photographs

- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

Servers:

- Staff are asked to save their documents in their folder or class resources folder of their server.
- Staff should not save documents on their desktop.
- Staff should be aware of GDPR, and should not save personal data unless needed. Once the date is over, for example a trip, data should be routinely cleansed.
- Staff should not share any electronic files from school.

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets)

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school server, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Our Outlook and networks are stored on the Cloud, and automatically update.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied
- All portable ICT devices must be locked up whenever you leave the school or are not in use.

The Gower School pupils are not allowed to have mobile phones in school, and occasionally Year 6 children, with advance permission from parents, which is included in the parent acceptable use policy, may bring them in if travelling to school alone. Pupil mobile phones should not be used on the premises, but switched off when they arrive, and left with the Year Six teachers locked into their cupboard during the school day, however and mobile phones which are kept on site are at the risk of the individual pupil. The Gower School is not responsible for any devices lost by pupils. No personal mobile phones are to be used in the EYFS setting during the teaching day (See Safeguarding Policy).

Cyber-Bullying: is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Cyberbullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying must be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection procedures (see our Safeguarding Policy).

Types of cyberbullying: There are many ways of bullying someone online and for some it can take shape in more ways than one. Some of the types of cyberbullying are:

Harassment - This is the act of sending offensive, rude, and insulting messages and being abusive. Nasty or humiliating comments on posts, photos and videos on social media sites, chat rooms and gaming sites.

Denigration – This is when someone may send information about another person that is fake, damaging and untrue. Sharing photos of someone for the purpose to ridicule, spreading fake rumours and gossip. The photos can also be altered for the purpose of bullying.

Flaming – This is when someone is purposely using extreme and offensive language and getting into online arguments and fights. They do this to cause reactions and enjoy the fact it causes someone to get distressed.

Impersonation – This is when someone will hack into someone's email or social networking account and use the person's online identity to send or post vicious or embarrassing material to/about others. They may also create fake accounts to cause hurt and humiliation.

Outing and Trickery – This is when someone may share personal information about another or trick someone into revealing secrets and forward it to others. They may also do this with private images and videos too.

Cyber Stalking – This is the act of repeatedly sending messages that include threats of harm, harassment, intimidating messages, or engaging in other online activities that make a person afraid for his or her safety. The actions may be illegal too depending on what they are doing.

Exclusion – This is when others intentionally leave someone out of a group such as group messages, online apps, gaming sites and other online engagement.

Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

ICT-Based Sexual Abuse: The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

There are no circumstances that will justify adults possessing indecent images of pupils. Adults who access and possess links to such websites will be viewed as a significant and potential threat to pupils. Accessing, making and storing indecent images of pupils is illegal. This will lead to criminal investigation and the individual being barred from working with pupils, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with pupils. Adults must ensure that pupils are not exposed to any inappropriate images or web links. Where indecent images of pupils or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Chat Room Grooming and Offline Abuse: Staff need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous.

The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Communicating and educating parents/carers in online safety: Parents will be provided with a copy of the IT User Acceptance Policy, and parents of years 3 to 6 will be asked to sign it on their child's behalf. The Gower School recognises the crucial role that parents play in the protection of their children with regards to online safety. The school will also provide parents and carers with information through newsletters, website and Parents sessions.
Parents and carers are always welcome to discuss their concerns on E-Safety with the school, who can direct them to the support of our E-Safety officer if required. Parents and carers will be encouraged to support the school in promoting good E-safety practice.

Parental Involvement
We believe that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents' consent to images of their child being taken and used in the public domain (e.g., on school website) when they sign the Acceptance of Place form.
- The school disseminates information to parents relating to E-Safety where appropriate in the form of posters, school website information, parents workshops and talks.

Taking and Storing Images of Pupils Including Mobile Phones (See Appendix 1): The Gower School provides an environment in which pupils, parents and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined in appendix 1 of this policy. This prevents staff from being distracted from their work with pupils and ensures the safeguarding of pupils from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

Our school embraces the benefits of using technology to communicate with parents, to share their child's activities and progression through photos and film imagery. This might be via the secure website My Montessori Child (available for all children 0-5 years), through our school website (promotional purposes and celebrating successes via the newsfeed, and for our online diary on the school Facebook page for example match results, Special Mentions, competition results, activities and celebrations).

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.

Use of photographs and films of children
At all times the school has an obligation to protect the interests and wellbeing of children, and all activities including taking and use of photographs comply with this commitment.

- When photographs or film clips of children are made available on Facebook, Twitter, YouTube or similar services, the names of the children are never used. Many competition entries now require a film clip uploaded to YouTube, and we do not put the child's full name on this.
- If a child is named on the school website or similar, no photograph will be displayed.
- Photographs of children record them successfully undertaking normal school activities, or celebrating their participation in external events. Photographs will not be used when they could bring the child into disrepute.
- Photographs of children will never be taken when they are not fully clothed.
- The school regularly reviews its procedures to ensure that use of photographs and films complies with up to date good practice. From time to time the school also runs information events for parents about good practice in use of the internet in relation to children.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a Mobile Phone Policy, which includes:

- The commitment to keep the pupils safe.
- How we manage the use of mobile phones at The Gower School taking into consideration staff, pupils on placement, volunteers, other professionals, trustees, visitors and parents/carers.
- How we inform parents/carers, visitors and other professional of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Policies.

Consent of Adults Who Work at the School

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If staff use a machine which is not routinely connected to the school network, they must make provision for regular virus updates through our IT team.
- If staff suspect there may be a virus on any school ICT equipment, they must stop using the equipment and inform a member of the SLT who will contact Compatibility immediately on 01892 665 326. Compatibility will advise of what actions to take and be responsible for advising others that need to know.

Security

- The school gives relevant staff access to the network and specific files on the network
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- SLT have identified relevant responsible persons as defined in the guidance documents https://www.islingtoncs.org/node/7905
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff must avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Information Asset Owner (IAO): Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. The IAO will be able to identify across the organisation:

- what information is held, and for what purposes
- what information needs to be protected how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

However, it is clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data amount to gross misconduct or even legal action.

E-mail: The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

Managing e-mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Staff must inform (the E-Safety Officer or line manager) if they receive an offensive e-mail
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section
-
- E-mailing Personal, Sensitive, Confidential or **Classified Information**
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

Receiving e-mails

- Check your e-mail regularly
- Never open attachments from an untrusted source; Consult your network manager first

E-mailing Personal, Sensitive, Confidential or Classified Information

Where your conclusion is that e-mail must be used to transmit such data:

- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Please read in conjunction with 'Internet Access Security' and EYFS E-Safety – Internet

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Principal's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- School internet access is controlled by the Sophos software and regular checking.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the E-Safety Officer or member of SLT or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from Principal
- If there are any issues related to viruses or anti-virus software, the Principal and the IT support company, Compatibility should be informed

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking and online games websites to pupils within school

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Principal
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Back up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote backups should be automatically securely encrypted.

Online Learning Tools:

Purple Mash

Children in Year 2 – Year 6 take part in weekly computing lessons using the Purple Mash. This has Units of work that are worked on throughout the year. We endeavour to send our staff on Purple Mash training at the start of the year. Each year, Online Safety is one of the units of work that is undertaken by each year group.

Atom Learning

In Upper School, each child has an Atom Learning account so that they can take part in English, Maths, Non Verbal and Verbal Reasoning lessons heading towards the 11+.

Google Classroom

Every child at The Gower School is given a personal Google Classroom account. This is used for uploading homework, assignments and newsletters etc. When we were in lockdown, children's work was uploaded here for teachers to mark as well.

E-Safety FAQs

For more information relating to E-safety procedures, refer to the E-Safety Frequently Asked Questions (FAQ) in Appendix 2. It covers the following topics on the relevant page as follows:

1 How will the policy be introduced to pupils? How will staff be consulted and made aware of this policy? How will complaints regarding Internet use be handled? How will parents' support be enlisted?

2 Why is the use of Internet and ICT important? How is the safe use of ICT and the Internet promoted? How does the Internet and use of ICT benefit education in our school? How will pupils learn to evaluate Internet content?

3 How is filtering managed? How are emerging technologies managed? How to react to misuse by pupils and young people

4 How is printing managed? What are the categories of Cyber-Bullying? What are the pupil rules?

5 What has research into Cyber Bullying found? What is the impact on a child of ICT based sexual abuse? What is the impact on a child of ICT-based sexual abuse? How do I stay secure on the Internet? Why is promoting safe use of ICT important? What does the school's Mobile Phone Policy Include?

6 Where can we learn more about Prevent? What do we have to do?

7 Do we have to have a separate *Prevent* Policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?

8 What training must we have? What are the potential legal consequences if we do not take the *Prevent* duty seriously? What are the rules for publishing content online?

Appendix 1 – Parents, volunteers and visitors photographing pupils

The Gower School provides an environment in which pupils, parents and staff are safe from images being recorded and inappropriately used. The growth of hand-held mobile technology and interconnectivity has implications for the safety of pupils, so in order to reflect the policy on safeguarding and child protection, upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined below. This includes where pupils are on school trips or residential. Neither are volunteers or visitors permitted to take photographs or recordings of the pupils. Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of pupils. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in school.

Parental use of mobile phones/cameras whilst on the school grounds

The Gower School allows parents to take photos of their own children at organised events such as a school performance, sporting event or celebration of learning. We will remind audiences of this at the start of each event, where practicable. Staff will also remind parents regularly of our school policy with regard to mobile phone use with the following statement when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g. a family album) and so are exempt from the Data Protection Act 1998. Please be aware these images (which may include other pupils) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of the Act." If parents wish to make or take an emergency call whilst on school grounds, they may use the office and the school phone.

Parents are welcome to take photographs of their own child taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events. Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts. We always print a reminder in the programme of events where issues of copyright apply. Additionally, the school records images of pupils, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph professionally events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of pupils while performing and disturbance within the audience.

When pupils join The Gower School, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld, this must be made clear when the consent form is returned to school so that photographs/videos are not published of the individual child concerned. The pupils take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents are welcome to take photographs of these memorable events, which may include groups of pupils. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents. Wherever possible, parents who take photographs of groups of children who are in the care of the school should gain consent first, ensuring that once any photographs are taken, they are stored safely and not posted to social media. The school recognises that it cannot police parents taking photographs of pupils who are outside school grounds and not in the school's care, however posting such pictures online may be in breach of the Data Protection Act 1998 without consent of all people within the photograph.

Appendix 2: *E-Safety FAQs*

How will the policy be introduced to Pupils?

- Rules for Internet access will be posted in all rooms where computers are used
- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access
- A module on responsible Internet use will be included in the PSHE programme covering both home and school use.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Pupils will be made aware of the acceptable use of technology and sign upon enrolment

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security
- Security strategies will be discussed at staff meetings.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as USB sticks, SD Cards and Hard Drives to carry work smust be kept confidential by staff and not used in public computers.
- Files held on the school network will be regularly checked
- All network system and administration passwords are to be recorded by the IT Department and kept in a secure place with regular updates

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the 'Responsible Internet Use' statement included in the staff handbook before using any Internet resource in school.
- All new staff will be taken through the key parts of this policy as part of their induction.
- All staff including teachers, learning support assistants and support staff will be provided with the School E-Safety Policy and have its importance explained as part of the child protection training requirement.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.
- Breaching this E-Safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
- Staff will read and sign *Staff Code of Conduct for ICT*- prior to using school ICT equipment in the school
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a member of the Senior Leadership Team.
- Complaints of Internet misuse will be dealt with by the Principal.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Policy and procedures.
- Pupils and parents will be informed of the complaint procedure.
- Parents and Pupils will need to work in partnership with staff to resolve issues.
- As with drug issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the responsible Internet use policy in newsletters, the parent portal and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach will be encouraged with parents and could include information booklets, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- We will maintain a list of e-safety resources for parents.
- Parents will be invited to attend an e-safety workshop annually.

Why is the use of Internet and ICT important?

Not only is familiarity with the use of ICT equipment a core requirement, but the efficient use of the equipment and available resources is also considered key – for example, the use of email for efficient communication and the correct use of the Internet for research. Staff across the school are making increased use of ICT, which benefits not only the quality of teaching and support services but also their professional development. It is equally important that staff are properly equipped and supported to make the most efficient use of ICT resources. In particular, ICT is extremely beneficial in engaging our pupils, who have learning and physical disabilities. It can also help them to access parts of the curriculum, which they might not otherwise be able to engage with.

All pupils deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" ICT facilities including online resources and services. Internet use is a part of the statutory curriculum and a necessary tool for staff and Pupils. The school has a duty to provide Pupils with quality Internet access as part of their learning experience. In order for the school to maintain such an environment for learners (pupils and adults) everybody must be aware of the need to ensure on-line protection (e-safety) and subsequently understand the principles of this policy and the expectations of school practice as documented below.

How is the Safe Use of ICT and the Internet Promoted?

The Gower School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community. The Gower School has in place an Internet firewall, Internet content filtering and antivirus software, and various IT security policies, which help to ameliorate the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe and The Gower School will further promote safe use of ICT and the Internet by educating pupils and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly. The school will ensure that the use of Internet derived materials by staff and Pupils complies with copyright law. The Gower School will help pupils to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our PSHEE and SMSC provision. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferInternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)

How does the Internet and use of ICT benefit education in our school?

- Pupils learn effective ways to use ICT and the Internet including safe and responsible use.
- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils worldwide.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with Local Authority and DfE
- Support of the wider curriculum through the use of word processing, spreadsheet and presentation tools, specialist applications, and the use of the Internet for research purposes.

How will Pupils learn to evaluate Internet content?

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the teacher, E-Safety Officer or SLT.
- Staff and Pupils must ensure that their use of Internet derived materials complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright.

How is Filtering Managed?

Having Internet access enables pupils to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. All unsuitable websites will be filtered and automatically blocked by our security systems and will not be made accessible to pupils. In addition, pupils' usage of our network will be continuously monitored. Compatibility will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of pupils. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

At The Gower School we believe that the benefits to pupils having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of pupils along with The Gower School share the responsibility for setting and conveying the standards that pupils will follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide pupils towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio.

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, they must report it to the E-Safety Officer, or teacher immediately.
- The school will take every step to ensure that appropriate filtering systems are in place to protect pupils from unsuitable material and the methods used will be reviewed regularly.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk).

How are Emerging Technologies Managed?

ICT in the 21st Century has an all-encompassing role within the lives of pupils and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by pupils may include:

- The Internet
- E-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Social media
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com / http://www.facebook.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com,http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'Internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

How to React to Misuse by Pupils and Young People

• **Step 1:** Should it be considered that a child or young person has deliberately misused ICT, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.

• **Step 2:** If there are to be further incidents of misuse, the child or young person will be suspended from using the Internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with a senior administrator and the most appropriate course of action will be agreed.

• **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

How is Printing Managed?
The use of the ICT printers may be monitored on an individual basis to encourage careful use of printing resources. As well as being a significant capital cost, the consumables (ink, laser printer toner and drums, and paper) associated with printing represent one of the most expensive ongoing costs associated with ICT. Whilst the school would not wish to discourage the proper use of printers, it is important to ensure that printing facilities are used efficiently and effectively. Pupils and staff are asked to take care not to waste printing resources, for example by using "Print Preview" to check work before sending it to the printer and by using colour print only when necessary.

General Housekeeping:
The ICT equipment used by the school represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order. In addition, the ICT resource is finite e.g. computers can run out of disk space; users should be encouraged to think about the amount of file storage they use and the need to keep it well organised. The school does not currently operate a quota system for disk space or mailboxes, but will consider doing so should the need arise.
The following will apply:

- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy.
- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

What are the Pupil Rules?

- Do not use ICT without permission.
- Food and drink must not be consumed near any computer equipment anywhere in the school.
- Do not move about the room while seated on a chair.
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.
- Computer faults should be promptly reported to the Senior Management or Compatibility. Please do not attempt to repair them yourself.
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at the workstation.

At the end of a session:

- Log off/shut down according to instructions.
- Replace laptops as directed.
- Wind up and put away any headsets.

What has Research into Cyber Bullying Found?
Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyberbullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyberbullying is done by pupils in the same class or year group and although it leaves no visible scars, cyberbullying of all types can be extremely destructive.

- Between a fifth and a quarter of pupils have been cyberbullied at least once over the previous few months.
- Phone calls, text messages and email are the most common forms of cyberbullying.
- There is more cyberbullying outside school than in.
- Girls are more likely than boys to be involved in cyberbullying in school, usually by phone.
- For boys, text messaging is the most usual form of cyberbullying, followed by picture/video clip or website bullying.
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyberbullying.
- Website and text bullying are equated in impact to other forms of bullying.
- Around a third of those being cyberbullied tell no one about the bullying.

What is the impact on a child of ICT based sexual abuse?

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

How do I stay secure on the Internet?

- Do not type any personal details (including your name or email address) into a web site unless you are absolutely sure of the authenticity and trustworthiness of the associated company.
- The use of chat rooms is prohibited.
- The use of Instant Messaging is prohibited.
- The use of Internet-based email or newsgroups is prohibited except with the prior written approval of the principal.

Why is Promoting Safe Use of ICT Important?

The Gower School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community.

What does the school's Mobile Phone Policy Include?

- The commitment to keep the pupils safe.
- How we manage the use of mobile phones at The Gower School taking into consideration staff, pupils on placement, volunteers, other professionals, trustees, visitors and parents/carers.
- How we inform parents/carers, visitors and other professional of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Policies.

Prevent – Top ten FAQs

We are receiving a number of queries to the support@isi.net inbox concerning inspection expectations in relation to the *Prevent* strategy so it may be useful if we address the most frequently asked issues.

1. Where can we learn more about *Prevent*?

There are two key source documents for the *Prevent* strategy:

- Statutory guidance Revised Prevent duty guidance: for England and Wales Updated 1 April 2021
- The Prevent duty Departmental advice for schools and childcare providers (2015 DfE)

2. What do we have to do?

The over-arching legal duty is to **"have due regard to the need to prevent people from being drawn into terrorism"** and, in so doing, have regard to guidance issued by the Secretary of State. In summary, the national statutory guidance from the Home Office, and sector-specific advice from the Department for Education places the following expectations on schools:

Leadership:

- establish or use existing mechanisms for understanding the risk of radicalisation
- ensure staff understand the risk and build the capabilities to deal with it
- communicate and promote the importance of the duty; and
- ensure staff implement the duty effectively.

Train staff: ensure staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism; ensure staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism and are shared by terrorist groups; ensure staff know where and how to refer pupils and young people for further help.

Work in partnership: co-operate productively, in particular, with local *Prevent* co-ordinators, the police and local authorities, and existing multi-agency forums, for example Community Safety Partnerships; ensure that safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Partnerships.

Share information appropriately: ensure information is shared between organisations to ensure, for example, that people at risk of radicalisation receive appropriate support.

Risk Assess: assess the risk of pupils being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. This should be based on an understanding, shared with partners, of the potential risk in the local area or our school's particular circumstances. This means being able to demonstrate both a general understanding of the risks affecting pupils and young people in the area and a specific understanding of how to identify pupils who may be at risk and what to do to support them.

Build resilience to radicalisation: promote fundamental British Values through the curriculum and through social, moral, spiritual and cultural education; equip pupils with knowledge, skills and understanding to prepare them to play a full and active part in society; ensure your school is a safe place to discuss sensitive issues, while securing balanced presentation of views and avoiding political indoctrination.

Safeguard and promote the welfare of pupils: put in place robust safeguarding policies to identify pupils at risk, and intervene as appropriate by making referrals as necessary to Channel or Children's Social Care, for example.

Ensure suitability of visiting speakers: operate clear protocols for ensuring that any visiting speakers, whether invited by staff or by pupils themselves, are suitable and appropriately supervised.

IT policies: ensure pupils are safe from terrorist and extremist material when accessing the Internet in school, including by ensuring suitable filtering is in place. The DfE advises that Internet safety will usually be integral to the ICT curriculum and can also be embedded in PSHEE, for example. Every teacher needs to be aware of the risks posed by online activity of extremist and terrorist groups. It is for schools to use their own judgement to fill in operational detail about how best to implement the duty in the context of the level of risk in their locality as advised by their Local Safeguarding Partnerships or other local agencies and the assessed risks to their own pupils.

What IT filtering systems must we have?
No technical guidance has been prescribed concerning the levels of filtering which are to be considered appropriate. This means that schools have discretion as to how they approach this aspect of the prevent duty. Keeping safe on-line is as much about educating pupils to think critically and about appropriate behaviour on-line as technical solutions.

What is the definition of a visiting speaker?
There is no definition of a visiting speaker. Schools should exercise their own reasonable judgement to determine who is a visiting speaker.

Do we have to check all our visiting speakers?
Schools must ensure all visiting speakers are suitable. There is scope for local discretion as to how. For example, a school could choose to check all speakers or to check all those whom risk assessment indicates warrant closer attention. The over-arching strategy should be recorded in the written protocol mentioned above.

What checks must we run on visiting speakers?
The means by which schools ensure the suitability of their speakers are not prescribed (except in the event that they happen to come within any of the usual categories in the Independent School Standards and Keeping Children Safe in Education, such as "staff"). Schools need not confine their approach to the usual formal checks; Internet searches, for example, may sometimes be more instructive than formal vetting checks.

What training must we have?
As a minimum, schools should ensure that the Designated Safeguarding Lead undertakes Prevent awareness training and is able to provide advice and support to other members of staff on protecting pupils from the risk of radicalisation. Schools should consider and arrange further training in the light of their assessment of risks.

What are the potential legal consequences if we do not take the *Prevent* duty seriously?
Where the Secretary of State is satisfied that a school has failed to discharge the duty under the Prevent strategy to have regard to the need to prevent people from being drawn into terrorism, the Secretary of State may give directions to the school to enforce performance of the duty. A direction can be enforced by court order.

What are the rules for publishing content online?

- Staff or pupil personal contact information will not be published on the school website. The only contact details given on our website will be the school address and telephone number.
- Pupil's full names will not be used anywhere on the school website or other on-line space.
- We may use photographs of pupils or their work when communicating with parents and the wider community, in newsletters and in the school prospectus.
- Photographs will be checked to ensure that they are suitable (photos of pupils in swimwear would be unsuitable).