Online 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 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 Miss Emma Gowers (Principal/Proprietor). 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:

Miss Emma Gowers
Principal and Proprietor

Date reviewed: May 2026
Date of next review: May 2027

This policy was last reviewed by the Principal/Proprietor and Senior Leadership Team (SLT) in May 2025 and will next be reviewed no later than May 2026 or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

1. Aims and Objectives

It is the duty of The Gower School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;

- Music/video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the IT Acceptable Use Policy for all staff, visitors and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Prevent
- Staff Code of Conduct;
- Behaviour Policy
- Data Protection Policy and Privacy Notice
- PSHE / RSE Policy

At The Gower School, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- "staff" includes teaching and non-teaching staff and volunteers;
- "parents" includes pupils' carers and guardians; and
- "visitors" includes anyone else who comes to the school.

Both this policy, and the Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, The Gower School has considered the "4Cs" outlined in KCSIE 2024, which are content, contact, conduct and commerce as the key areas of risk.

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

However, The Gower School recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's Behaviour Policy and/or Safeguarding Policy as is appropriate in the circumstances.

3. Roles and responsibilities in relation to online safety

All staff and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in in line with the Safeguarding and Child Protection Policy.

3.1. Principal/Proprietor and the Senior Leadership Team

The Principal/Proprietor is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

3.2. The Designated Safeguarding Leads (DSLs)

The DSLs take the lead responsibility for Safeguarding and Child protection at The Gower School. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSLs will ensure that this policy is upheld at all times, working with the Principal/Proprietor and Senior Leadership Team, Online Safety Co-ordinator and IT service providers to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSLs will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSLs will work closely with the Online Safety Coordinator and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The Principal/Proprietor, Online Safety Coordinator and the school's IT service provider will review filtering and monitoring reports and ensure that termly checks are properly made of the system.

3.3. Online Safety Coordinator

The DSLs have delegated day to day responsibilities relating to online safety to the school's Online Safety Coordinator, Mrs Tajana Baldwin. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The Online Safety Coordinator will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the DSLs.

3.4. IT service provider

The Gower School's IT service provider has a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system and its data. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Online Safety Coordinator.

3.5. Teaching and support staff

All staff are required to sign and return the IT Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and the Principal/Proprietor and Senior Leadership Team as appropriate.

3.6. Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy.

3.7. Parents and carers

The Gower School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The Gower School will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

4. Filtering and Monitoring

In general:

The Gower School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The Online Safety Coordinator will check once per week that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. During weekly Senior Leadership meetings the Principal/Proprietor, the DSLs and Online Safety coordinator will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The Gower School's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content and adult content. If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact the Online Safety Coordinator and DSLs for their consideration.

The Gower school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. In line with the school's Data Protection Policy and/or Privacy Notice, the Online Safety Coordinator/IT service provider will monitor the logs. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the Online Safety Coordinator, their Head of Department and the DSL if they are teaching material which might generate unusual internet traffic activity.

Regularly, the Deputy Teacher will test the effectiveness of the firewall by searching for a range of sites which we believe the firewall should protect us from accessing.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the head of their department/Online Safety Coordinator and the DSL if they believe that appropriate teaching materials are being blocked.

Pupils:

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the appropriate teacher who will notify the Online Safety Coordinator/DSL. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work/research purposes, pupils should contact the Online Safety Coordinator for assistance.

Additional guidance on "appropriate" filtering and monitoring can be found at: UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring

The UK Safer Internet Centre produced a series of webinars for teachers on behalf of the Department. These webinars were designed to inform and support schools with their filtering and monitoring responsibilities and can be assessed at https://saferinternet.org.uk/blog/filtering-and-monitoring-webinars-available

In Forms 5 and 6, we use the Safe Skills website (https://safeskillsinfo.lgfl.net) to test the children's knowledge and identify gaps in learning where we need to direct our teaching.

5. Education and training

5.1. Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school.

All staff receive regular information and training (at least annually) on online safety issues in the form of staff training days and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

5.2. Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The Gower School provides opportunities to teach pupils about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE and RSE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. Upper school pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities. Pupils can report concerns to their teacher in the first instance who will then inform the DSL/Online Safety Coordinator.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding/Anti Bullying/Sanctions Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach their teacher, the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

5.3. Parents

The Gower School seeks to work closely with parents and guardians in promoting a culture of 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 Gower 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. We will also provide parents and carers with information through newsletters, our website and School Cloud. The Gower School will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

6. Use of school and personal devices

Staff

The Gower School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the Staff Code of Conduct and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at The Gower School are permitted to bring in personal devices for their own use. Staff are not allowed to use their personal devices around the children during the working day. They may use such devices in the main staffroom, during break-times and lunchtimes.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, Acceptable Use, Staff Code of Conduct.

Staff at The Gower School must 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).

Staff must ensure that their screen display is out of direct view of any third parties when accessing personal, sensitive, confidential or classified information. They must ensure that they lock their screen before moving away from their computer during the normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

Pupils

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they must be kept switched off and signed in at the school office at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The Gower School mobile technologies made available for pupil use, including laptops, tablets, cameras, etc. are stored in a locked cupboard. Access is available via teachers. Members of staff should ensure that each device is returned after each use by a pupil.

Pupils are responsible for their conduct when using school issued or their own devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Policy.

The Gower School recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with Head of Nursery or Head of Operations & School SENCO to agree how the school can appropriately support such use. They will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

7. Online Communications

Staff

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent/carer who has left the school within the past 12 months using any personal email address or SMS/WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents/carers. Under no circumstances may staff contact a pupil or parent/carer using a personal telephone number, email address, or other messaging system nor should pupils, parents be added as social network 'friends' or similar.

Staff must immediately report to the DSL/Principal the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Online Safety Coordinator/IT Staff.

8. Use of social media

Staff

Staff must not access social networking sites, any website or personal email which is unconnected with school work or business from school devices or whilst teaching/in front of pupils. Such access may only be made from staff members' own devices whilst away from the children.

When accessed from staff members' own devices/off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of The Gower School in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring The Gower School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;

- using social media to bully another individual; or
- posting links to or endorsing material which is discriminatory or offensive.

- otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

Pupils

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. We expect pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The Gower School takes misuse of technology by pupils vary seriously and incidents will be dealt with under the Behaviour, Safeguarding and Child Protection and Anti-Bullying policies as appropriate.

Online Learning Tools that children access

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.

Scratch

Scratch is a visual, block-based programming language and online community designed by MIT for children aged 8 to 16. It is used in Upper School Computing Lessons to teach the basics of coding and computational thinking

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+. Homework can also be set on here.

Linguscope

Linguscope is a popular, award-winning online language learning platform designed primarily for primary and secondary schools. It provides interactive multimedia resources, games, and printable worksheets to help educators teach up to 16 languages across elementary, beginner, and intermediate levels. There is one login that the whole school can use.

Edclub

Edclub (best known for its program TypingClub) is an interactive, web-based educational platform designed to teach users how to touch type. It helps individuals type efficiently using all ten fingers without looking at the keyboard.

9. Data protection

Personal data will be recorded, processed, transferred and made available according to GDPR. The Gower 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 and must be encrypted.

Staff and pupils are expected to save all data relating to their work to their school laptop/PC or to the school's central server as per the IT Acceptable Use Policy.

Staff should also be particularly vigilant about scam/phishing emails (and similar) which could seriously compromise The Gower School's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the Principal/Proprietor in accordance with the Data Protection Policy and IT Acceptable Use Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Principal/ Proprietor and Online Safety Coordinator.

It is important to remember that any information held on The Gower School systems, hardware or used in relation to school business may be subject to The Freedom of Information Act.

10. Password security

Staff have individual school email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every [6] months;
- not write passwords down; and
- not share passwords with other pupils or staff.

11. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites).

12. Artificial Intelligence

Generative AI refers to technology that can be used to create new content based on large volumes of data that models have been trained on from a variety of works and other sources. ChatGPT and Google Bard are generative artificial intelligence (AI) tools built on large language models (LLMs).

Tools such as ChatGPT and Google Bard can:

- answer questions

- complete written tasks
- respond to prompts in a human-like way

Other forms of generative AI can produce:

- audio
- code
- images
- text
- simulations
- videos

AI technology is not new and we already use it in everyday life for:

- email spam filtering
- media recommendation systems
- navigation apps
- online chatbots

However, recent advances in technology mean that we can now use tools such as ChatGPT and Google Bard to produce AI-generated content.

Generative AI tools are good at quickly:

- analysing, structuring, and writing text
- turning prompts into audio, video and images

When used appropriately, generative AI has the potential to:

- reduce workload across the education sector
- free up teachers' time, allowing them to focus on delivering excellent teaching

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. The content produced by generative AI could be inaccurate, inappropriate, biased, taken out of context and without permission and out of date or unreliable

In particular, pupils should not use these tools to answer questions about health/medical/wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff/DSL.

13. Misuse

The Gower School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate we will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL and Principal/Proprietor. They may then seek assistance from the Child Exploitation and Online Protection, the LADO, and/or its professional advisers as appropriate.

The Gower School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour policies.

14. Complaints

As with all issues of safety at The Gower School, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the Principal/Proprietor in the first instance, who will liaise with the Senior Leadership Team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.