SH29 - Online Safety Policy

Contents

Key Details

Designated Safeguarding Lead: Jayne Gosling

Named Governor with lead responsibility: Elisabeth Lawrence

Date written: (January 2023)

Date agreed and ratified by Governing Body: (June 2023)

Date of next review: (June 2024)

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure

Introduction

Online safety at Glyne Gap School

Glyne Gap is a school for pupils aged between 2-19 years of age with severe and profound learning disabilities. Many of our pupils have other additional needs including physical, medical, sensory and autistic spectrum condition. We recognises that statistically children with Special Educational Needs and Disabilities (SEND) are usually more vulnerable online. However for many pupils at Glyne Gap School their disability can also act as a risk reduction/ protective factor.

Physical access/ Supervision: For many pupils their physical disability provides a protective factor. This is because many of our pupils require full adult support/ physical prompt to access the internet, social media or mobile devices. Therefore they would never be alone with any device. The pupils who have the physical ability (e.g. dexterity and fine motor skills) to access online devices are always supervised by members of staff while online at school, so there is lower likelihood of them being exposed to online risks/ harm during the school day.

Significantly delayed cognitive development: For some of our pupils their significant learning disability can at times, act as a protective factor from online harms. Some pupils may come across inappropriate content, but wouldn't have the cognitive development to understand the meaning, associate emotions or recognise this as potentially harmful.

We recognise the invaluable role parents and carers play in contextual safeguarding. We work closely with identified pupils and their families to ensure that pupils are taught the skills to stay safe online, in a personalised approach that is meaningful and helpful to them.

Glyne Gap School takes online safety very seriously to ensure that all pupils remain safe online both now and in their future. Safeguarding on and offline is everyone's responsibility and we uphold the mindset 'It could happen here'.

1. Policy Aims

This online safety policy has been adapted by Glyne Gap School, involving staff, pupils and parents/carers, building on the East Sussex County Council/The Education People online safety policy template, with specialist advice and input as required.

It takes account of the DfE statutory guidance Keeping Children Safe in Education 2022, Early Years and Foundation Stage and the East Sussex Safeguarding Children Partnership procedures.

The purpose of Glyne Gap School online safety policy is to:

Ensure that the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices

Provide staff with the overarching principles that guide our approach to online safety

Identify approaches to educate and raise awareness of online safety throughout the community.

Ensure that, as a school, we operate in line with our values and within the law in terms of how we use online devices.

Four areas of risk:

Glyne Gap School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

2. Policy Scope

- Glyne Gap School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- Glyne Gap School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Glyne Gap School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as pupils, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school but is linked to member of the school.
- In this respect the school will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of school. Action can only be taken over issues covered by the published Behaviour Policy

2.1. Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Curriculum Guideline 2 (CG2): Safeguarding and Child Protection Policy
- Curriculum Guideline 7 (CG7) Supporting Positive Attitudes and Good Behaviour Policy
- School Handbook 17 (SH17) Staff behaviour Policy
- Schools code of conduct.
- Curriculum Guideline (CG17): Relationship and Sex Education Policy
- Curriculum Guideline 6 (CG6): Personal, Social and Health Education
- Core skills for functionality (CG8)

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; Glyne Gap School will review this policy at least annually
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head teacher (Kirsty Prawanna) will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding (Elisabeth Lawrence) will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Jayne Gosling) has lead responsibility for online safety.
    - Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.
- Glyne Gap School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1. The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with Schools ICT to monitor the safety and security of our systems and networks; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).
- Ensure that online safety is embedded within curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Recognise that a one size fits all approach may not be appropriate for all children and a more personalised or contextualised approach to online safety is used for pupils at Glyne Gap School.
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school or college safeguarding approach.
- Support the DSL and any deputies by ensuring they have appropriate time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Audit and evaluate online safety practice annually, to identify strengths and areas for improvement.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.

4.2. The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the schools safeguarding responsibilities and that a coordinated approach is implemented.
- Liaise with staff (especially class teacher, admin team, IT technicians, and senior mental health leads) on matters of safeguarding that include online and digital safety.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep pupils safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns to the Governor responsible for Safeguarding (Elisabeth Lawrence)
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (Once a term) with the governor with a lead responsibility for safeguarding including online safety.

4.3. It is the responsibility of all members of staff to:

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use agreement
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Proactively monitor the use of digital technologies, I pads, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.

- Take personal responsibility for professional development in this area.
- Ensure that students are 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.
- Reinforce the school's online safety messages when teaching lessons online

4.4. It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures *(eg password protected)* to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team, as well as, the settings Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

4.5. It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Understand the importance of good online safety practice out of school, and understand that this policy covers their actions outside of school if related to their membership of the school.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6. It is the responsibility of parents and carers to:

- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1. Education and engagement with pupils

- The School has developed online safety curriculum modules to raise awareness and promote safe and responsible online behaviour at school and at home amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes internet access.

  - Including online safety in Personal, Social, and Health Education (PSHE), Relationships and Sex Education (RSE) and goals and IEPs.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will support pupils to read and understand the acceptable use rules (appendix 1) in a way which suits their age and ability by:
  - Displaying acceptable use posters in all rooms with internet access.
  - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology.
  - Providing online safety education for pupils who have the cognitive ability to understand this topic meaningfully.
  - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2. Vulnerable Pupils

- Glyne Gap School recognises that all pupils at our school could be more vulnerable online due to their Special Educational Needs and Disabilities (SEND).
- Glyne Gap School also recognises other factors which could make pupils more vulnerable online. This may include, but is not limited to children in care, children with or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Glyne Gap School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- For the majority of pupils at Glyne Gap a personalised approach to online safety would be most appropriate. This will involve online safety being imbedded in goals, IEPs and super goals.
- For the small group of pupils who have academic capacity and physical ability to access technologies independently, they will be taught online safety through the schools modules/ schemes of work.
- When implementing an appropriate online safety policy and curriculum Glyne Gap School will seek input from specialist staff as appropriate, including The Head of Faculty (Sarah Tidmarsh) and Assistant Headteacher responsible for curriculum (Barbara Clarke).

5.3. Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with ALL members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This is part of our annual whole school safeguarding refresher training.
- This will cover the potential risks posed to pupils (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.

- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the community.

5.4. Awareness and engagement with parents and carers

- Glyne Gap School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats.
    - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, and sports days.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Glyne Gap School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1. Classroom Use

- Glyne Gap School uses a wide range of technology. This includes access to:
    - Computers, laptops and ipads.
    - Internet which may include search engines and educational websites
    - Games consoles and other games-based technologies
    - Digital cameras.
- All setting owned devices will be used in accordance with our acceptable use documents and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. For example *Google Safe Search or CBBC safe search*.
- We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.
    - **Key Stage 2**
        - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.
    - **Key Stage 3, 4, 5**
        - Pupils will use age-appropriate search engines and online tools.
    - Pupils will be appropriately supervised when using technology, according to their ability and understanding.

7.2. Managing Internet Access

- All staff and pupils will read and sign an acceptable use agreement before being given access to our computer system, IT resources or internet.

7.3. Filtering and Monitoring

7.3.1. Decision Making

- Glyne Gap School Leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The School Leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2. Filtering

- Education broadband connectivity is provided through The South East Grid for Learning (SEGfL) Internet Service for Schools and Academies purchased via East Sussex County Council.
- A key benefit of the SEGfL service is Enhanced Internet Content Filtering from Smoothwall:-
    - It exceeds the requirements for the provision of 'Appropriate Filtering' as required by Keeping Children Safe in Education.
    - Smoothwall blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
    - Smoothwall also blocks all sites on the Internet Watch Foundation (IWF) list.
    - Smoothwall Cloud enables managed school devices to be filtered when offsite.
    - BYOD devices brought into School can also be filtered by central Smoothwall appliances.
- If pupils discover unsuitable sites, they will be required to:
    - Turn off screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputies) and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Sussex Police or CEOP.

7.3.3. Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - Notification from Smoothwall of any breaches.
    - DSL keeps a log of all breaches with any actions taken
- If a concern is identified via monitoring approaches we will:
    - *Be reported to the DSL or head teacher immediately.*

- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4. Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

7.5. Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.

- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1. Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 2022, some pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private. List of login details are held by teacher.
- We require all users to:
    - Use strong passwords for access into our system.
    - Change their passwords every three months.
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

7.6. Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or pupils personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7. Publishing Images and Videos Online

Images are only shared on the school website and parent/carer approval is always obtained.

7.8. Managing Email

- Access to our email systems will always take place in accordance with data protection legislation.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately inform (Jayne Gosling, DSL) if they receive offensive communication, and this will be recorded in our safeguarding files/records.

- We have a dedicated email for reporting Safeguarding issues. (DSL@glynegap.org)This inbox is managed by a designated and trained staff (Toni Muceku)

7.8.1. Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

7.8.2. Learner email

For a small cohort of pupils who are learning to independently use emails:

- Pupils will use provided email accounts for educational purposes.
- Pupils will sign an acceptable use policy as part of the curriculum and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9. Please note that the school does not use video calls with pupils.

7.10. Please note that the school does not use online Learning Platforms.

7.11. Please note that we do not use an online app to record and share pupil's progress.

8. Social Media

8.1. Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Glyne Gap School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Glyne Gap School community are expected to engage in social media in a positive, safe and responsible manner.
    - All members of Glyne Gap School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control pupil and staff access to social media whilst using school provided devices and systems on site.
    - The use of social media during school hours for personal use is not permitted.
- Concerns regarding the online conduct of any member of Glyne Gap School community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our, behaviour and child protection policies.

8.2. Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Glyne Gap School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Headteacher.
    - If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing school networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the DSL (or deputies).

8.3. Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for pupils under this age.
- Any concerns regarding pupil's use of social media will be dealt with in accordance with existing policies.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools and the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.
    - To remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.

8.4. **Please note we do not have an official school Social Media site.**

9. Use of Personal Devices and Mobile Phones

- Glyne Gap School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

9.1. Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such Behaviour, Safeguarding and Staff Code of Conduct.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of Glyne Gap School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of Glyne Gap School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pool.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community.
- All members of Glyne Gap School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2. Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time. (not on their person)
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching time, unless permission has been given by the Head teacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the DSL or Headteacher.
- Staff will not use personal devices:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - Directly with pupils and will only use work-provided equipment during lessons or educational activities.
- If a member of staff breaches our policy, action will be taken in line with our SH17 code of conduct.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3. Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Glyne Gap School expects pupils' personal devices and mobile phones to be kept in a secure place, switched off, kept out of sight during lessons and while moving between lessons. (unless the use of the device is 'part of the learning')
- If a pupil needs to contact his/her parents or carers they will be allowed to use the class phone or their personal device by agreement.
- Parents are advised to contact their child via the schools office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.

- Mobile phones or personal devices will not be used by pupils during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If a pupil breaches the policy, the phone or device will be confiscated and will be held in a secure place.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
    - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day.
    - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4. Visitors' Use of Personal Devices and Mobile Phones

- We expect Parents/carers and visitors (including volunteers and contractors) to use their mobile devices in a respectful manner while on the school premises.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or Headteacher of any breaches our policy.

9.5. Officially provided mobile phones and devices

- Classes will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.
- Class mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- Safeguarding concerns and incidents, at level 3 or 4 on the Continuum of Need, should be reported to Single Point of Advice in line with East Sussex Safeguarding and Child Protection model policy.

- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Standards and Learning Effectiveness Service Safeguarding Team.
- Where there is suspicion that illegal activity has occurred contact the Sussex Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or headteacher will contact Sussex Police first to ensure that potential investigations are not compromised.

10.1. Concerns about Pupils' Welfare

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputies) will record these issues in line with our child protection policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the East Sussex Safeguarding Children Partnership thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2. Staff Misuse

- Any complaint about staff misuse will be referred to the head teacher, in accordance with the allegations policy.
- For any allegations regarding a member of staff's online conduct a consultation will be sort with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1. Online Sexual Violence and Sexual Harassment between Children

- Glyne Gap School has accessed and understood sexual violence and sexual harassment between children in schools and colleges (2021) guidance and part 5 of Keeping Children Safe in Education September 2022.
- Glyne Gap School recognises that sexual violence and sexual harassment between children can take place online and our staff will maintain an attitude of 'it could happen here'. Examples may include; non-consensual sharing of nudes and semi-nudes images and videos, sharing of unwanted explicit content, up-skirting, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- Glyne Gap School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Glyne Gap School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Glyne Gap School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between

children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our Safeguarding Policy.
    - If content is contained on pupil's electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate supports (update IPA/ risk reduction Plan) in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Sussex Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2. Youth Produced Sexual Imagery ('Sharing nudes and semi nudes')

- Glyne Gap School recognises youth produced sexual imagery (known as "sharing nudes and semi nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people,.
- Glyne Gap School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi nudes (or sexting) by implementing preventative approaches, via a range of age and ability appropriate educational methods (goals/ IEPs)
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is
    - a clear need or reason to do so in order to safeguard the child or young person. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.– **in most cases, images or videos should not be viewed**

  - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant East Sussex Safeguarding Child Partnership's procedures.
  - Ensure the DSL (or deputy) responds in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance.
  - Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of pupils involved; including carrying out relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Children's Social Care and/or the Police, as appropriate.
  - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
  - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
  - Consider the deletion of images in accordance with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
  - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3. Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines)

- Glyne Gap School will ensure that all members of the community are aware of online child sexual abuse including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Glyne Gap School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  - Act in accordance with our child protection policies and the relevant East Sussex Safeguarding Child Partnership's procedures.
  - If appropriate, store any devices involved securely.

  - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
  - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
  - Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Standards and Learning Effectiveness Service and/or Police.
- If pupils at other settings are believed to have been targeted, the DSL (or deputy) will contact the Police.

11.4. Indecent Images of Children (IIOC)

- Glyne Gap School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police and/or the Standards and Learning Effectiveness Service.
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant East Sussex Safeguarding Child Partnership's procedures.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Sussex police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or deputy DSL) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
  - Ensure that the DSL (or deputy DSL) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
  - Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - Quarantine any devices until police advice has been sought.

11.5. Cyberbullying

- All staff at Glyne Gap School understand that children are capable of abusing their peers online. Cyberbullying, along with all other forms of bullying, will not be tolerated here.
- Full details of how we will respond to cyberbullying are set out in our Behaviour and Safeguarding Policies.

11.6. Cybercrime

- Glyne Gap School will ensure that all members of the community are aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
- If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme.
- We will seek advice from Cyber Choices, 'NPCC- When to call the Police' and National Cyber
- Security Centre.

11.7. Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Glyne Gap School and will be responded to in line with existing policies, including Safeguarding and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Sussex Police.

11.8. Online Radicalisation and Extremism

- Glyne Gap School will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation
- We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site. (Through our daily smooth wall filtering system and weekly reviews at the safeguarding Team meeting)

- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the head teacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Useful Links for Educational Settings

East Sussex Support and Guidance:

- East Sussex County Council Early Years Support & Intervention Team
  - Call: 01323 463026
  - Email: childcare.support@eastsussex.gov.uk
- If you are concerned about a child in East Sussex contact SPOA (Single Point of Advice) on 01323 464222 or 0-19.SPOA@eastsussex.gov.uk
- Standards and Learning Effectiveness Service (SLES): SLES.Safeguarding@eastsussex.gov.uk
  East Sussex Schools ICT Service: Richard May
  Richard.May@eastsussex.gov.uk

East Sussex Support and Guidance for Educational Settings

- https://czone.eastsussex.gov.uk/safeguarding/
- https://czone.eastsussex.gov.uk/safeguarding/support-for-safeguarding-in-colleges-schools-and-early-years-settings/

East Sussex Safeguarding Children Partnership

- www.sussexchildprotection.procedures.org.uk/

Sussex Police:
www.sussex.police.uk

- For non-urgent Police contact 101
- If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Online Safety Toolkit: Online Safety - Czone (eastsussex.gov.uk)

Blank page

Appendix 1 – Glyne Gap Online Safety Policy - Acceptable use rules for pupils

This is how we stay safe when we use computers at school and at home:

- I will ask an adult if I want to use the computers / devices and will only use it when they are with me;
- I will only use activities that an adult has told or allowed me to use;
- I will keep information about me safe;
- I will not share my password;
- I will be kind to others online when I am sending messages;
- I will ask for help from an adult if I am not sure what to do or if I think I have made a mistake;
- I will tell an adult if I see something that upsets me on the screen or if I am worried;
- I know that if I break these rules, I might not be allowed to use the computers / devices;

Blank page

Appendix 2 – Glyne Gap Online Safety Policy - Social Media Guidance

Do not accept friend requests from pupils on social media

10 rules for staff on social media

1. Change your display name - use your first and middle name, use a maiden name, spell your surname backwards, use a nickname, or use a contraction

2. Change your profile picture to something unidentifiable, or if not, ensure the image is professional

3. Check your privacy settings regularly

4. Be careful about tagging other staff members in images or posts

5. Don't share anything publicly that you wouldn't be just as happy showing your pupils

6. Don't use social media sites in school hours

7. Don't make comments about your job, your colleagues, your school or your pupils online - once it's out there, it's out there

8. Don't associate yourself with your school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)

9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address / mobile number) is able to find you using this information

10. Consider uninstalling social media apps from your phone, The app recognises wi-fi connections and makes friend suggestions based on who else uses the same wi-fi connection (such as parents or pupils)

Check your privacy settings

Facebook

- Change the visibility of your posts and stories to 'Friends', rather than 'Public'. Otherwise pupils and their families may be able to see your posts and pictures you've been tagged in, even if you haven't accepted a friend request or they're not on Facebook
- Don't forget to check your old posts and photos – see Facebook's privacy support page for step-by-step instructions on how to do this
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
- Prevent search engines from indexing your profile so people can't search for you by name – see Facebook's step-by-step instructions
- Remember, some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender
- Google your name to see what information about you is visible to the public

Instagram

- Change your profile visibility from the default 'Public' setting to 'Private'. Otherwise pupils and their families will be able to see your posts, reels, locations, and who you are following and are followed by. Go to the Instagram Help Centre for support with your privacy settings
- If a pupil or parent followed you before you changed your privacy settings, block them to prevent them seeing your posts
- Be careful about giving third-party apps or websites access to your Instagram account, and check app privileges in your phone to see if any apps currently have access. Sharing your information can put your account at risk and make you visible on search engines, even if you have set your account to 'Private'.
- Remember, some information is always public; your username, your bio and your profile picture
- Google your name to see what information about you is visible to the public

Twitter

- If you have a Twitter account specifically for or about teaching, make sure you don't include identifying information about yourself or your school. Use a nickname, for example 'Miss M'
- Change the visibility on your birth date to 'You follow each other' to prevent pupils and parents seeing this personal information. See Twitter's profile visibility guidance for more support
- Remember, your username, biography, location, website and profile picture are always public and can be seen by pupils and parents, even if they don't follow you and you have protected your tweets
- Protect your tweets by checking the box in the 'Audience and tagging' section of your privacy settings. This will mean only your approved followers can see your tweets
- Google your name to see what information about you is visible to the public

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, remind them of your school's social media policy (if you have one), or tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify your senior leadership team or headteacher about what is happening

A parent adds you on social media

- It is at your discretion, in accordance with your school's social media policy, whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore a message, consider drafting a stock response (either individually or as a school) to let the parent know why you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- Do not retaliate or respond in anyway
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or relevant social network and ask them to remove it
- If the perpetrator is a current school pupil or staff member, the school's own mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address their concerns, address any reasonable complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or someone from the school should consider contacting the police

Blank page

Appendix 3 – Glyne Gap Online Safety Policy - Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school′s reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Blank page

Appendix 4 – Glossary of Terms

TERM	DEFINITION
Antivirus - delete	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.