Online Safety Policy

June 2022

School Aims

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Members
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk: -

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as 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 – personal online behaviour that increases the likelihood of, or causes, harm, such as 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 scam

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out Golden Hill.

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Head Teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

The Management committee has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation. The Management committee will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding leads (DSL).

The Member who oversees online safety is **Mrs Joanne Bowker: Chair of Golden Hill's Management Committee.**

All Members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Head Teacher:

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The online safety lead works in conjunction with the Head Teacher to monitor online safety within school.
- The Head Teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made. Whether this is against a pupil or another member of the school community *(see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority procedures).*
- The Head Teacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head Teacher will receive regular monitoring reports from the Online Safety Lead.

Designated Safeguarding Lead (DSL):

- Details of the school's DSL responsibilities are set out in Golden Hill's Safeguarding and Child Protection policy as well as relevant job descriptions.
- Our DSLs are: Mrs Allison Collinge (Main DSL and Head Teacher), Mrs Sarah Barrett (In - school Deputy Head Teacher and Back Up DSL), Ms Sue Payne (Deputy Head Teacher/ GHIST Lead and Back up DSL)
- The Online Safety Lead is Linda El Kout.
- The DSLs in conjunction with the Online Safety Lead takes responsibility for online safety in school, in particular:
    - Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
    - Address any online safety issues or incidents

- Manage all online safety issues and incidents in line with Golden Hill's Safeguarding and Child Protection policy
- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with Golden Hill's Behaviour Management policy
- Update and deliver staff training on online safety
- Liaise with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the Management committee

Online Safety Lead: Additional Responsibilities

- Leads the Online Safety Group
- Has a leading role in establishing and reviewing the school online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with Golden Hill's technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with Online Safety Member to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meetings of the Management Committee.
- Reports regularly to Senior Leadership Team

Technical Staff

Ed-IT maintain technical responsibilities for the school and include:-

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Local Authority's online safety technical online guidance.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. The Online Safety Lead: Linda El Kout will check the filtering system every week and Ed-It will generate a filtering report every half term.
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Head Teacher and Senior Leaders; Online Safety Lead, DSL (where appropriate) for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

All Staff and Volunteers

All staff, including contractors and agency staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSLs to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

The Online Safety Group

- The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Management committee.
- Members of the Online Safety Group will assist the Online Safety Lead and Head Teacher with:
    - the production/review/monitoring of Golden Hill's online safety policy/documents.
    - mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
    - monitoring network/internet/filtering/incident logs
    - consulting stakeholders – including parents/carers and the pupils about the online safety provision

Pupils

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement (see Appendix 3 & 4)
- KS2 pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (as covered in the online safety curriculum)
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying (as covered in the online safety curriculum)
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / carers are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 2)

Parents / carers can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Healthy relationships – Disrespect Nobody

Guides to social media / apps / games - Netaware

Keeping children safe online – Internet Matters

- Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy when relevant and will be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Teaching Online Safety

- Pupils will be taught about online safety as part of the curriculum (discretely, through computing and through PSHE / RSE)
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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

1. Use technology safely and respectfully, keeping personal information private

2. Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

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

3. Use technology safely, respectfully and responsibly

4. Recognise acceptable and unacceptable behaviour

5. Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

6. That people sometimes behave differently online, including by pretending to be someone they are not

7. That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

8. The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

9. How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

10. How information and data is shared and used online

11. What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

12. How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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

Training

Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents / carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Seesaw messages
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications (as referenced on the school's online safety page on our website)

The Wider Community

The school will provide opportunities for members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents
- The school website will provide online safety information for the wider community

Staff and Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.

- This online safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Lead will provide advice/guidance/training to individuals as required

Members

Members should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents (this may include attendance at parental/ carers briefings).

Technical – Filtering and monitoring

Golden Hill will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username by Ed-It who will keep an up to date record of users and their usernames. Users are responsible for the security of their logins.
- The “master/administrator” passwords for the school systems, used by the IT technician must also be available to the Head Teacher / Computing Subject Leader and kept in a secure place (e.g. school secure key safe)
- The IT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Specific accounts have been created for supply teachers, trainee teachers, etc, and temporary accounts can be made for specific visitors when needed.
- An agreed policy is in place that allows forbids staff from downloading executable files and installing programmes on school devices. Staff request for apps / programmes to be downloaded by the administrator. Administrator will further check suitability / appropriateness and then make the decision.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

- Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.
- All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should is an integral part of the school's online safety education programme.
- The school acceptable use agreements for staff, pupils and carers will give consideration to the use of mobile technologies.

Golden Hill allows:

	School Devices (iPads, laptop)			**Personal Devices**		
	School owned for single user	**School owned for multiple users**		**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes		No	Yes	Yes
Full network access	Yes	Yes		No	No	No
Internet only	Yes	Yes		No	Yes	Yes
Any network access	Yes	Yes		No	No	No

School owned/provided devices:

- Staff have access to teacher laptops, Surface Pros and iPads to use within teaching and learning.
- Devices can be used in school to support teaching and learning and can be taken out of school for planning / school trips, etc.
- Devices are password protected with school managed passwords (GDPR compliant)

- Photographs that are taken on staff iPads for evidence will be uploaded to the secure public server and then deleted.
- Photographs will not be posted on social media (unless photograph consent sought from parents).
- All devices are connected to the school internet and are filtered by the school filtering system: **Surf Protect**
- Devices are wiped if a teacher leaves school.
- The Ed-IT technician is responsible for the management of devices, installation of apps and changing of settings and technical support.
- Staff have signed the AUP with regards to their usage of devices.
- Staff have received and are receiving ongoing training to use the devices and are aware of policies linked to device use.

Personal devices

- Staff and visitors are allowed to use mobile devices in school
- Staff are able to use mobile devices during break times only
- Staff are given access to the internet through their device. Visitors will not have this access.
- Devices are not given access to networks.
- Staff will not be allowed to use personal devices for school business except for school email accounts
- The school reserves the right to take, examine and search users' devices in the case of misuse – this is also included in Golden Hill's Behaviour Management policy
- Technical support is not available for personal devices
- Taking/storage/use of images on personal devices is forbidden
- The school takes no liability for loss/damage or malfunction following access to the network. However, it is unlikely that any personal devices have access to the network
- Visitors will be informed of school requirements during their induction. Access to the school internet is only given upon request.
- Pupils are educated about the safe and responsible use of mobile devices as part of the online safety curriculum.

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 online-bullying 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. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press

- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Personal Data

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- it has a Data Protection Policy
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents and volunteers with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to

see to have a copy of the personal data held about them (subject to certain exceptions which may apply).

- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers. it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults			Students/Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	
Mobile phones may be brought to the school/academy	Yes			No				
Use of mobile phones in lessons	No			No				
Use of mobile phones in social time				No				
Taking photos on personal mobile phones/cameras	No			No				
Use of other personal mobile devices e.g. tablets, gaming devices	No			No				
Use of personal email addresses in school or on school network				No				
Use of school email for personal emails	No			No				

Use of messaging apps on personal devices	No			No				
Use of social media	No			No				
Use of blogs	No			No				

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users should be aware that email communications are monitored. Users must immediately report, to the nominated person – in accordance with the school policy, 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.
- Any digital communication between staff and pupils or parents/carers (email, Seesaw, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- All staff will only use school ipads or laptops to access Seesaw
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Protecting Professional Identities

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
Golden Hill provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures
- Personal Use:
- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Monitoring of Public Social Media:
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process
- The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

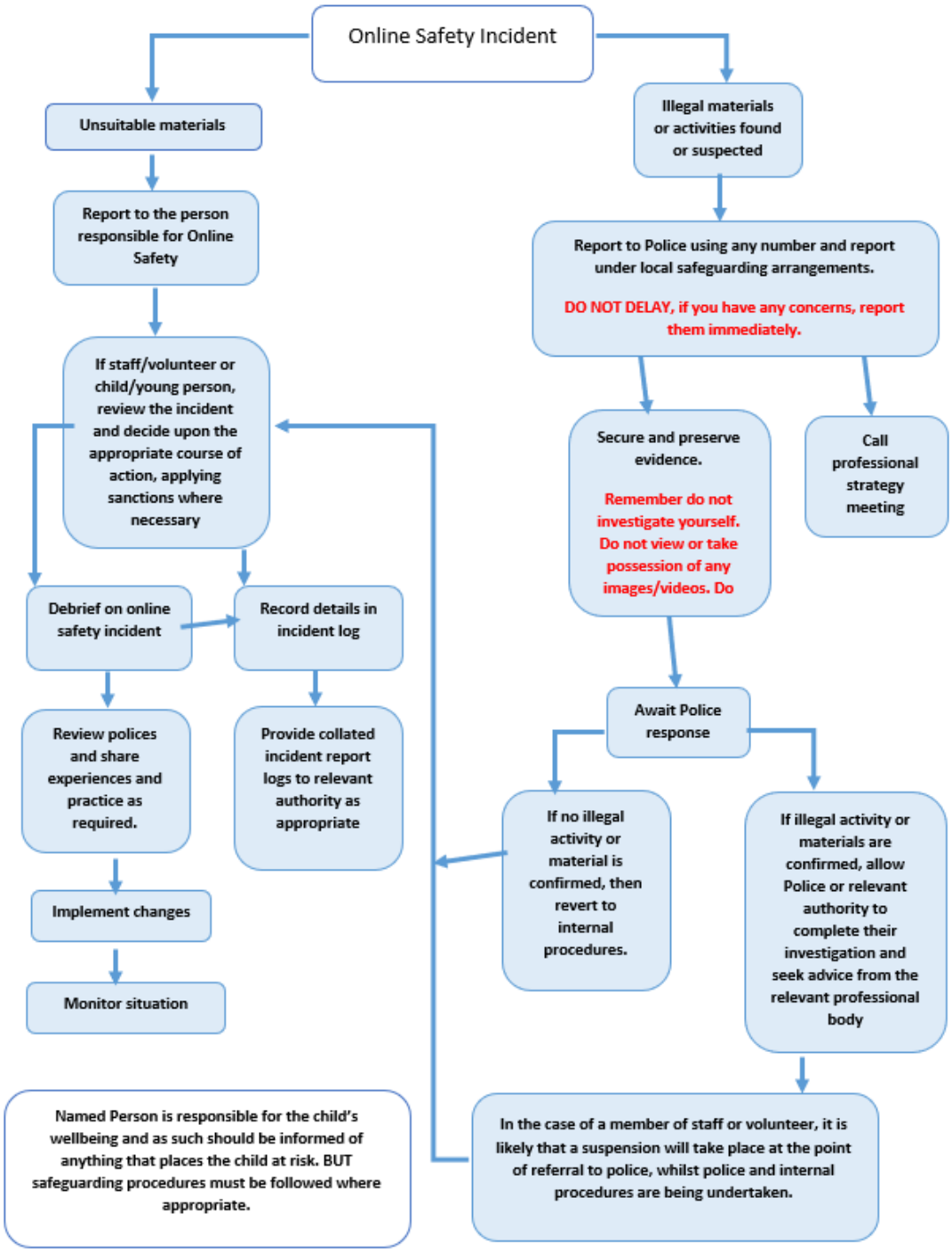
- Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.
- The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination					x
	threatening behaviour, including promotion of physical violence or mental harm					x
	Promotion of extremism or terrorism					x
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						x
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)						x
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	

Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright					x
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					x
Creating or propagating computer viruses or other harmful files					x
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

- This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).
- If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

- It is important that all of the above steps are taken as they will provide an evidence trail for the school possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.
- It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible

in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

	Actions/Sanctions								
Students/Pupils Incidents	Refer to class teacher	Refer to Deputy Head Teacher	Refer to Head Teacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	x							x	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device			x		x	x		x	
Unauthorised/inappropriate use of social media/ messaging apps/personal email			x		x	x		x	
Unauthorised downloading or uploading of files			x		x	x		X	
Allowing others to access school network by sharing username and passwords	x					x		x	
Attempting to access or accessing the school network, using another pupil's account	x					x		x	
Attempting to access or accessing the school network, using the account of a member of staff	x		x			x		x	x
Corrupting or destroying the data of other users	x		x		x	x		x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			x			x			x
Continued infringements of the above, following previous warnings or sanctions			x	x		x	x		x

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x		x	x			x
Using proxy sites or other means to subvert the school's filtering system			x	x	x	x			x
Accidentally accessing offensive or pornographic material and failing to report the incident			x		x	x		x	
Deliberately accessing or trying to access offensive or pornographic material			x	x	x	x	x		x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x	x	x	x	x		x

Actions/Sanctions

Staff Incidents	Refer to Deputy Head	Refer to Head Teacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email		x			x	x		
Unauthorised downloading or uploading of files		x			x	x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x			x			x
Careless use of personal data e.g. holding or transferring data in an insecure manner		x			x	x		
Deliberate actions to breach data protection or network security rules		x	x	x	x			x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x	x			x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x	x	x			x
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		x			x			x

Actions which could compromise the staff member's professional standing		x	x		x			x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x		x			x
Using proxy sites or other means to subvert the school's filtering system		x	x		x			x
Accidentally accessing offensive or pornographic material and failing to report the incident		x	x		x			x
Deliberately accessing or trying to access offensive or pornographic material		x	x		x			
Breaching copyright or licensing regulations		x			x	x		
Continued infringements of the above, following previous warnings or sanctions		x	x	x	x			x

Online Safety Policy Agreed: June 2022

Online Safety Policy Update: June 2024

Appendix 1

Golden Hill Short Stay School

Staff (and Volunteer) Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupil learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using the school systems

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Members / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read the Acceptable Use Policy and understand and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:.....

Signed:.....

Date…….

Appendix 2
Golden Hill Short Stay School
Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance the learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form
Parent/Carers Name: .....

Pupil Name: .....

As the parent/carer of the above pupils, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: ..... Date: .....

Appendix 3:- Use of Digital/ Video Images Agreement
Golden Hill Short Stay School

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and on Seesaw. Where an image is publicly shared by any means, only your child's first name/initials will be used.

The school will comply with the Data Protection Act and request parent's/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Digital/Video Images Permission Form

Parent/Carers Name:..... Pupil Name:.....

As the parent/carer of the above pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these digital/video images being used:	
• to support learning activities.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
• on the Seesaw app and the school website	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed:.....

Date: .....

Appendix 4:- Pupil Acceptable Use Policy – EYFS & KS 1 Agreement
Golden Hill Short Stay School

This Acceptable Use Policy
We endeavour to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

Please could parents/carers read and discuss this policy with their child to ensure they understand their roles and responsibilities when using technology at school and then sign for our school records.

This is how we stay safe at EYFS and KS1 when we use computers:

- I will ask a teacher or trusted adult if I want to use the computer.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer, ipads, laptops and other equipment.
- I will ask for help from the teacher or a trusted adult if I am not sure what to do or if I think I have done something wrong.
- I will tell the teacher or trusted adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use the computer/ipad/laptop again in the future

<u>Use of Seesaw</u>

- I will only use Seesaw app to complete work at home.
    - The adults at school may send work on Seesaw for you to send back to them
- My teachers and school adults will only use their school account to talk to myself and my adults
    - My teachers will use equipment that has been given to them by school where possible
    - My teachers will only answer between 8.45 – 5pm
    - Other adults (Head Teacher and deputy head) can see everything we post

<u>Data Protection and Security</u>

- Any personal information will be stored safely and will link to the school's Data Protection Policy
- All remote learning and any online communication will take place in line with current school confidentiality expectations as outlined in GDPR Policy.
- Seesaw will record my adults, my own and my teacher's activity
- Only adults and children at Golden Hill will be able to get onto Seesaw
- Access to Seesaw will be managed in line with current IT security expectations

Behaviour Expectations

- I am expected to behave like I do at school when using Seesaw. This means that if I am recording a voice note/video or photo, I will use appropriate words and behave as I would do in school. This also applies to typing comments, drawing etc on Seesaw.

Policy Breaches and Reporting Concerns

- If I make a wrong choice during my time of online learning at home, this will be reported to the Head Teacher
- The Head Teacher will decide what to do based on existing polices such as anti-bullying and behaviour
- Any Safeguarding concerns will be reported to Allison Collinge, Designated Safeguarding Lead, Sarah Barrett (Back up DSL) or Sue Payne (Back up DSL)

Signed (child) ……..

(Parent can sign on behalf of the child, having read the policy with the child)

Signed (parent/carer)……

Appendix 5:- Pupil Acceptable Use Policy – KS2 Agreement
Golden Hill Short Stay School

This Acceptable Use Policy

We endeavour to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the school's ICT resources in a responsible manner, to make sure that I keep myself and others safe whilst working online.

Personal Safety

- I will keep my passwords safe and will not use other people's passwords
- I will be aware of 'stranger danger', when working online
- I will not share personal information about myself or others when online.
- I will not upload any images of myself or of others without permission
- I will not arrange to meet up with people that I have communicated with online.
- I will immediately report any inappropriate material, messages I receive or anything that makes me feel uncomfortable when I see it online.
- I will report any bad behaviour by telling a responsible adults and learn about using the CEOP Report button
- I know that the school can look at my use of ICT and what I use online
- I understand that Golden Hill's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission
- I will not use any programs or software without permission
- I will not install programs or alter any computer/ipad settings

I understand that I am responsible for my actions, both in and out of school

- I understand that there will be consequences if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve the community (eg cyber-bullying, use of images or personal information)
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, there will be consequences for my actions. This may include loss of access to the school network, contact with parents and in the event of illegal activities, involvement of the police

Use of Seesaw

- I will only use Seesaw app to complete work at home.
    - The adults at school may send work on Seesaw for you to send back to them
- My teachers and school adults will only use their school account to talk to myself and my adults
    - My teachers will use equipment that has been given to them by school where possible

- My teachers will only answer between 8.45 – 5pm
- Other adults (Head Teacher and deputy head) can see everything we post

Data Protection and Security

- Any personal information will be stored safely and will link to the school's Data Protection Policy
- All remote learning and any online communication will take place in line with current school confidentiality expectations as outlined in GDPR Policy.
- Seesaw will record my adults, my own and my teacher's activity
- Only adults and children at Golden Hill will be able to get onto Seesaw
- Access to Seesaw will be managed in line with current IT security expectations

Behaviour Expectations

- I am expected to behave like I do at school when using Seesaw. This means that if I am recording a voice note/video or photo, I will use appropriate words and behave as I would do in school. This also applies to typing comments, drawing etc on Seesaw.

Policy Breaches and Reporting Concerns

- If I make a wrong choice during my time of online learning at home, this will be reported to the Head Teacher
- The Head Teacher will decide what to do based on existing polices such as anti-bullying and behaviour
- Any Safeguarding concerns will be reported to Allison Collinge, Designated Safeguarding Lead, Sarah Barrett (Back up DSL) or Sue Payne (Back up DSL)

Please complete the sections below, to show that you have read, understood and agree to the rules included in this Acceptable Use Agreement. If you do not sign and return the agreement, access will not be granted to school systems and devices.

I have read and understood the above and agree to follow these guidelines when

- I use the school systems and devices (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school

Name of pupil _____

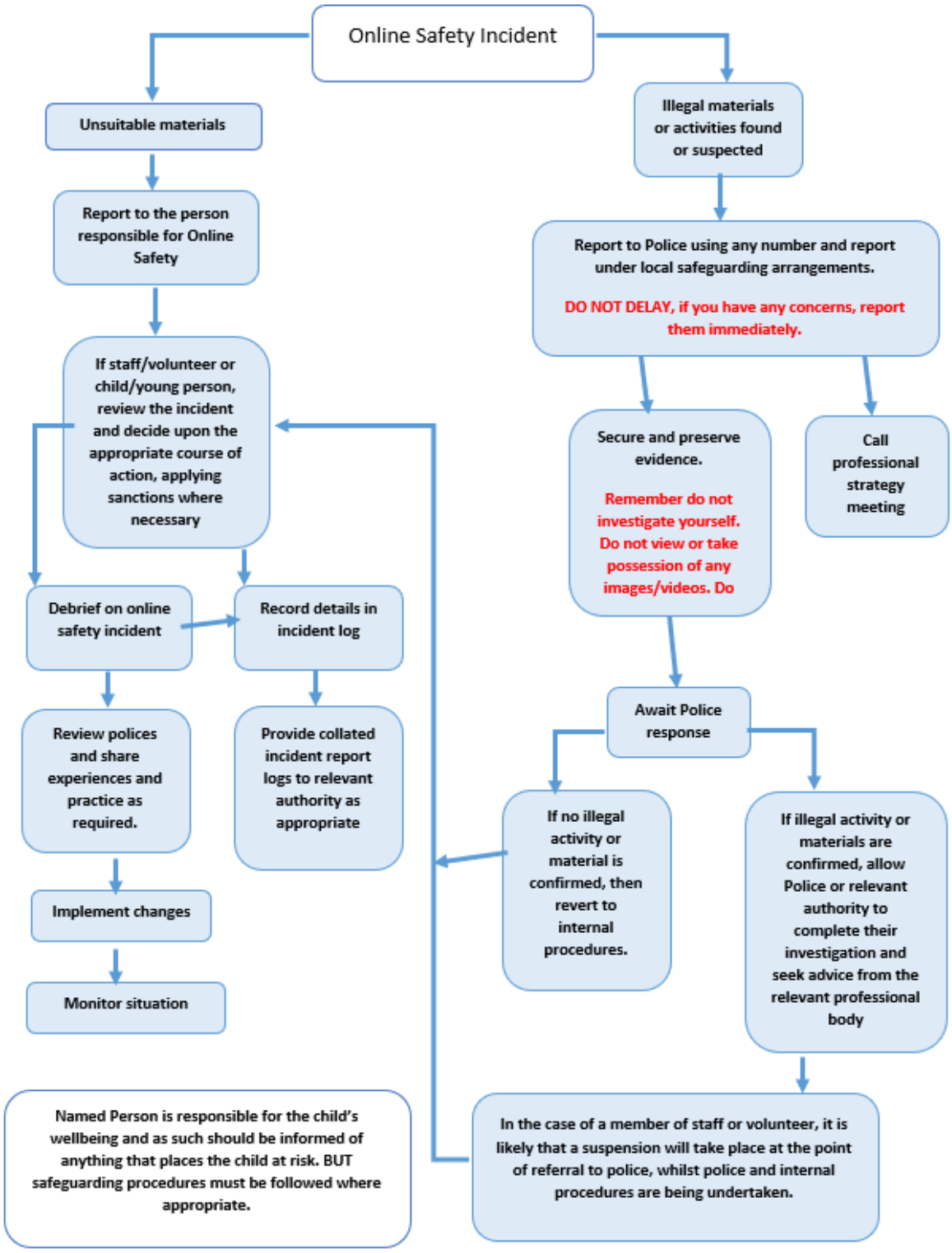
Pupil Signature: _____

Date: _____

Parent /Carer: _____ (to show awareness of school / home expectations)

Appendix 5

Responding to incidents of misuse – flow chart



Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....
Date: .....
Reason for investigation: .....
.....
.....

Details of first reviewing person
Name: .....
Position: .....
Signature: .....

Details of second reviewing person
Name: .....
Position: .....
Signature: .....
Name and location of computer used for review (for web sites)
.....
.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken	

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date
